Parcours de découverte du monde connecté

Objectifs :

Utiliser au mieux le monde connecté

Faire les bons choix pour s'équiper

Fabriquer ses propres objets connectés

G Leclercq

Version 1.16

2020

Table des matières

Index des figures

1 Introduction

Bienvenue dans ce parcours de découverte du monde connecté et de sa mise en pratique !

Le monde connecté prend de plus en plus de place dans notre vie. Il nous offre de plus en plus de services, par exemple :

Pour notre confort :

volets roulants automatiques, éclairage selon l'ambiance souhaitée, gestion du chauffage, robot aspirateur, préparation de notre liste de course, proposition de menus...

Pour notre santé : bracelets, montres connectés

Pour nos loisirs : Android TV, Google play, spotify...

Pour notre sécurité, l'aide à domicile par exemple.

Ce parcours de découverte du monde connecté comprend deux cours :

Pour le cours 1, Nous allons nous promener sur internet pour découvrir différents types de sites web. Nous allons découvrir la richesse des services qu'ils nous offrent. Nous allons également découvrir des sites dont le service est de faire des relations avec d'autres sites et avec nos appareils. Nous verrons comment mettre en place des relations afin d'obtenir des services personnalisés pour améliorer notre confort et notre sécurité. Par exemple : le soleil se couche alors déclencher la fermeture automatique des volets.

Pour le cours 2, nous verrons comment faire des projets basés sur l'utilisation de ces sites web publics et d'objets connectés.

Le cours 1 intitulé "**Découverte du monde connecté**" va nous permettre d'utiliser au mieux ce monde connecté et de faire les bons choix pour s'équiper.

Le cours 2 intitulé "**Ateliers objets connectés**" s'adresse aux plus curieux et va nous permettre de réaliser des projets basés sur l'utilisation de ces sites web publics et d'objets connectés. Ces objets connectés sont ceux qu'on trouvera dans le commerce ou qu'on fabriquera nous-mêmes.

Il y aurait tellement à dire qu'il va falloir que nous restions concentrés sur l'essentiel. Mon objectif n'est pas de tout détailler, mais de vous mettre en appétit. 😊
Si vous avez ensuite envie d'en savoir plus (et je suis convaincu que cela va arriver !), de nombreux cours d'approfondissement vous attendent ensuite au club!

Les objectifs de ces cours sont de vous permettre :

- **d'utiliser au mieux le monde connecté**
- **de faire les bons choix pour s'équiper**
- **de fabriquer vos propres objets connectés**

Ces cours s'adressent à toute personne curieuse et qui sait naviguer sur internet à partir d'un PC.

Voilà un programme court condensé et, je l'espère, alléchant ! Alors...Allons-y !

2 Cours 1 : Découverte du monde connecté

2.1 Les notions de base du monde connecté

L'objet de ce chapitre est de présenter les principales notions de base du monde connecté.

Nota : Ce chapitre est une adaptation des « cours informatiques gratuits et sans publicité » présenté sur le site : http://www.coursinfo.fr/decouverte/internet/.

Aujourd'hui le monde est connecté. Le média par excellence qu'il utilise est l'internet.

Dans ce cours, nous utilisons le terme «monde connecté» pour désigner l'ensemble des éléments qui le constituent : réseau internet, sites web, clients web.

Nous aborderons également les notions de base liées au service de chiffrement et à la protection de notre vie privée.

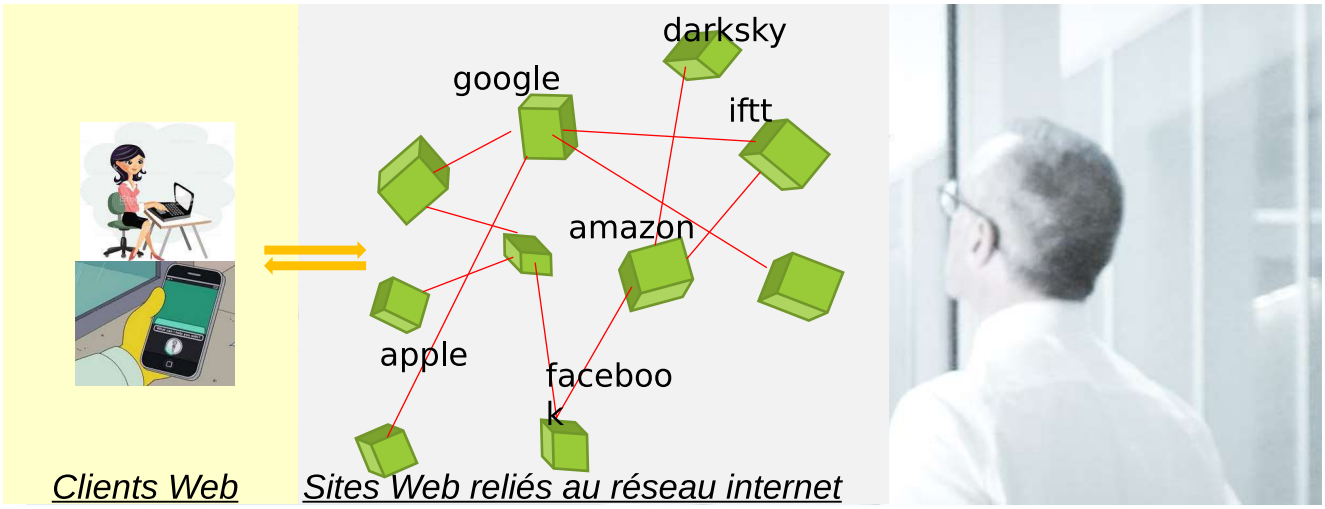


Illustration 1: Illustration du monde connecté

2.1.1 Le monde connecté c'est "l'internet" et "le web"

Dans le langage courant, les termes "web" et "Internet" sont souvent utilisés comme des synonymes. Pourtant, ils ne désignent pas la même chose et ne sont pas interchangeables.

2.1.1.1 L’internet est un réseau

Internet (contraction de **I**nter Network) est un réseau qui relie des machines entre elles à l'échelle du monde. Ce gigantesque réseau se compose de millions de réseaux publics et privés plus petits, par exemple des réseaux universitaires, gouvernementaux ou commerciaux.

Cette vaste infrastructure informatique repose sur le protocole de communication **I**P (pour **I**nternet Protocol), qui permet d'acheminer des données entre les machines via un maillage de serveurs et de routeurs.

L’internet permet de multiples usages comme le partage de fichiers, la messagerie instantanée, la téléphonie, l'envoi de courrier électronique, le web.

Le **réseau Internet** s’apparente au **réseau routier mondial** composé d’autoroutes, de routes nationales et départementales pour **relier les différents endroits du globe** entre eux !

Le Web s’apparente aux **boutiques de commerce et aux magasins** où l’on va faire ses courses ou encore aux **blibliothèques municipales** où on va consulter des livres.

2.1.1.2 Le web est la principale application d’internet

Le **web** (abréviation de World Wide Web ou toile mondiale) est un service d'**I**nternet parmi d'autres.

C'est la création du web par Tim Berners-Lee en 1989 qui a popularisé l'utilisation d'**I**nternet auprès du grand public, d'où la confusion qui existe encore entre ces deux termes.

Pour expliquer autrement la différence entre web et **I**nternet, on pourrait dire que **le web n'est pas l'Internet mais sa principale application**. Il s'agit d'un système de publication et de consultation de documents : des sons, des images et des textes comme l'article que vous êtes en train de lire...

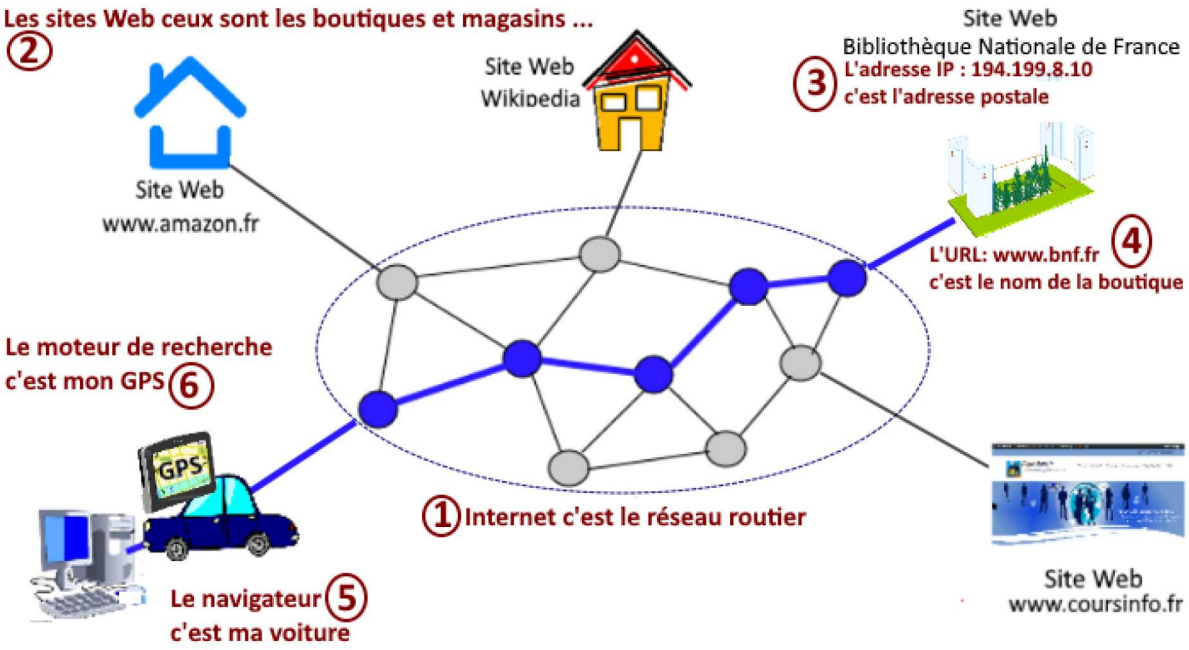


Illustration 2: L'internet c'est un réseau routier mondial

Internet c'est **l'équivalent du réseau routier mondial**

1.les **sites web** sont l'équivalent des **boutiques**, **magasins** et **bibliothèques** accessibles par le **réseau Internet.**

2.l'**adresse IP** c'est l'**adresse postale** de la **boutique.**
Exemple ***:*** *194.199.10.8 équivaut sur Internet à Quai François-Mauriac, 75706 Paris pour la BNF*

3.l'**URL** c'est le **nom** de la **boutique** (*l'enseigne*)
Exemple : www.bnf.fr équivaut sur Internet au nom (ou l'enseigne) de la Bibliothèque Nationale de France

4.le **navigateur** c'est la **voiture** pour me **déplacer** sur le **réseau Internet** et aller à la **boutique** de mon choix

5.le **moteur de recherche** c'est mon navigateur **GPS** qui m'aide à **trouver le chemin** pour aller à la boutique de mon choix.
Pour cela, je donne des **mots-clés** au **moteur de recherche** et il me renvoie une **liste de liens vers des sites** en **résultats. Je clique alors sur un des liens et j'arrive sur la boutique de mon choix.**

Ce système utilise les techniques de **l'hypertexte**, c'est-à-dire des hyperliens ou liens qui vous permettent de surfer d'une partie d'un document à une autre ou d'un document à un autre d'un simple double-clic.

Nota : L'internet est aussi utilisé par d'autres services que le web. Citons par exemple: la messagerie (exemple Messagerie Thunderbird), la Voix sur IP (Skype, Whatsapp), le streaming (Molotov), le peer to peer (bittorrent).

Exercice :

Sur le réseau internet, pouvez-vous citer les différents types de « véhicules » de caractéristiques différentes qu'on y voit circuler ?

2.1.1.3 Histoire de l'invention de l'internet et du web

L'Internet et le web , n'ont pas été inventées à la même époque.

Le réseau Arpanet (ancêtre d'Internet) a vu le jour **à la fin des années 1960** et a permis l'envoi du premier message électronique en 1972.

En revanche, il a fallu attendre les années **1989** et 1990 pour que les technologies à la base du web soient mises au point par des chercheurs du Cern : Tim Berners-Lee et Robert Cailliau.

2.1.1.4 Savoir se repérer dans le monde connecté

Quelques termes et illustrations pour se repérer....

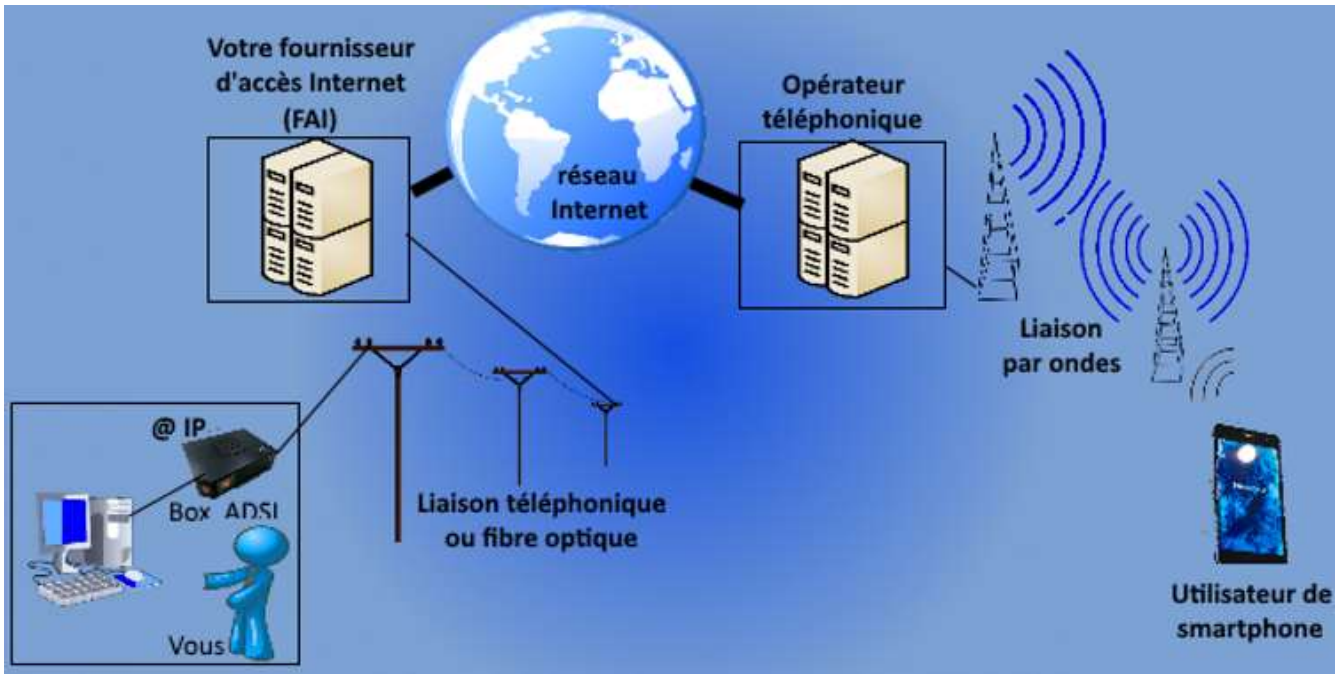


Illustration 3: Illustration physique de l'internet

Chaque personne possédant un **ordinateur, un smart phone,** une **box,** une **ligne téléphonique** ou **fibre optique** et **un numéro d'accès à l'internet** (@ IP) peut **se connecter** sur le réseau, recevoir et envoyer des informations instantanément (texte, sons, images) dans n'importe quelle partie du monde.

Principe :

- Les **ordinateurs** connectés à **Internet** doivent avoir **une adresse unique** (@ IP) pour être contactés : c'est *l'adresse IP*
- les **ordinateurs** doivent utiliser le **même langage : HTTP (pour le service Web)** pour communiquer entre eux**.**
- les **pages d'information** sont codés en langage **HTML** *(Hypertexte Marked Langage)*.

Des logiciels facilitent la lecture de ce langage HTML. Ce sont les **logiciels de navigation** ou **navigateur ;** voici quelques exemples **:**

- **Firefox** de Mozilla,
- **Opera** Opera Software,
- **Chrome** de Google,
- **Safari** d'Apple …

Les **Fournisseurs d'accès** sont des **sociétés** (*Orange, Free, SFR, Bouygues* ...) qui disposent d'un **serveur** (ordinateur capable de partager des informations et de connecter d'autres ordinateurs sur un réseau) et qui **ont loué un certain nombre de lignes** aux agences de téléphone (France Télécom en France) afin de permettre à des clients (entreprises, vous ou moi) qui disposent du matériel nécessaire de **se connecter sur le réseau Internet moyennant un abonnement**.
Lors de l'installation de votre connexion à l'Internet (installation de la « box » internet ou « routeur »), le **fournisseur d'accès vous alloue une adresse IP publique.**
Cette adresse IP peut être permanente ou dynamique.
Par exemple, l'adresse IP publique fournie par les opérateurs Knet ou Free est permanente.
L'adresse IP publique par l'opérateur orange est dynamique, c'est à dire modifiable par l'opérateur après plusieurs jours.

Exercices :
1) Quel est l'intérêt et/ou le désavantage d'avoir une adresse IP publique permanente ?
2) Quel est l'intérêt et/ou le désavantage d'avoir une adresse IP publique dynamique ?

Qu'est ce qu'un réseau domestique ?

Ref

Le réseau domestique (on dit également ''réseau local'') désigne toute l'installation informatique interconnectée chez soi. Voir illustration ci-dessous.

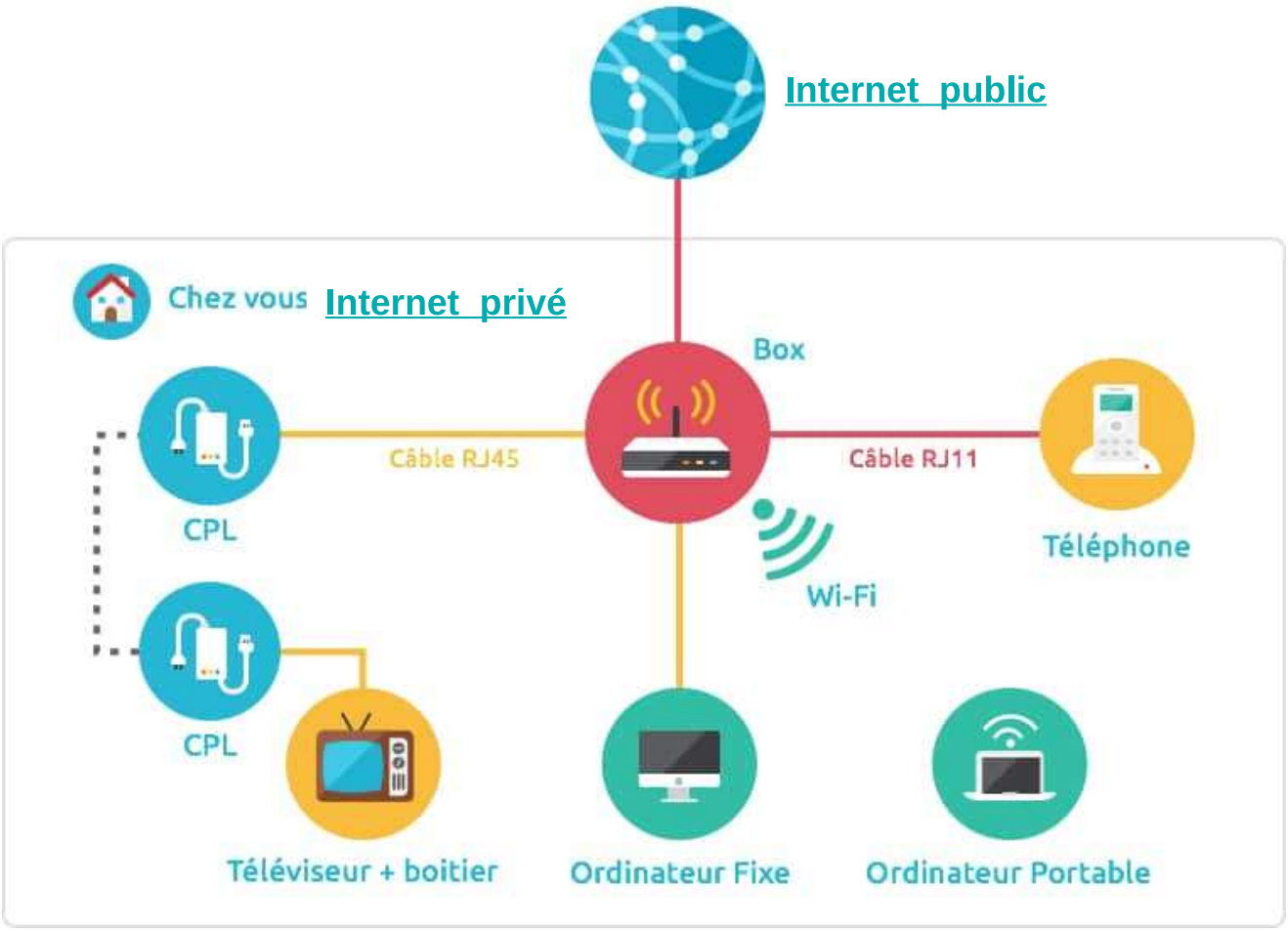


Illustration 4: Réseau domestique

Le réseau domestique est un internet privé sécurisé par la box

Le réseau domestique illustré en figure ci-dessus est en fait composé d'ordinateurs connectés sur un internet privé.

Ces ordinateurs sont : la Box, le boîtier sur lequel est connecté la télévision, l'ordinateur fixe, l'ordinateur portable, le boîtier téléphone (non représenté, inclus dals la box ou relié à la box) sur lequel est relié le téléphone.

La Box joue en particulier un rôle de « pare-feu » (firewall). Elle permet à ces ordinateurs situés sur l'internet privé de se connecter à des ordinateurs (serveurs) situés sur l'internet public. Par contre, elle interdit à un ordinateur public de se connecter sur un ordinateur de l'internet privé.

Qu'est-ce qu'une adresse IP ?

Sur Internet, les **ordinateurs** communiquent entre eux grâce à un ensemble de protocoles dont le **protocole IP** (Internet Protocol). Ce protocole utilise des **adresses numériques** que l'on appelle **adresses IP** (@ IP).

Chaque ordinateur, chaque site Web possède sa propre adresse IP.
Ainsi, le site web : **www.coursinfo.fr** a pour adresse IP : **213.186.33.16**
Par exemple, **194.199.8.10** est **l'adresse IP de la Bibliothèque Nationale de France (BNF)**.
=> L'adresse IP c'est l'équivalent de l'adresse postale (Quai François-Mauriac, 75706 Paris pour la BNF).

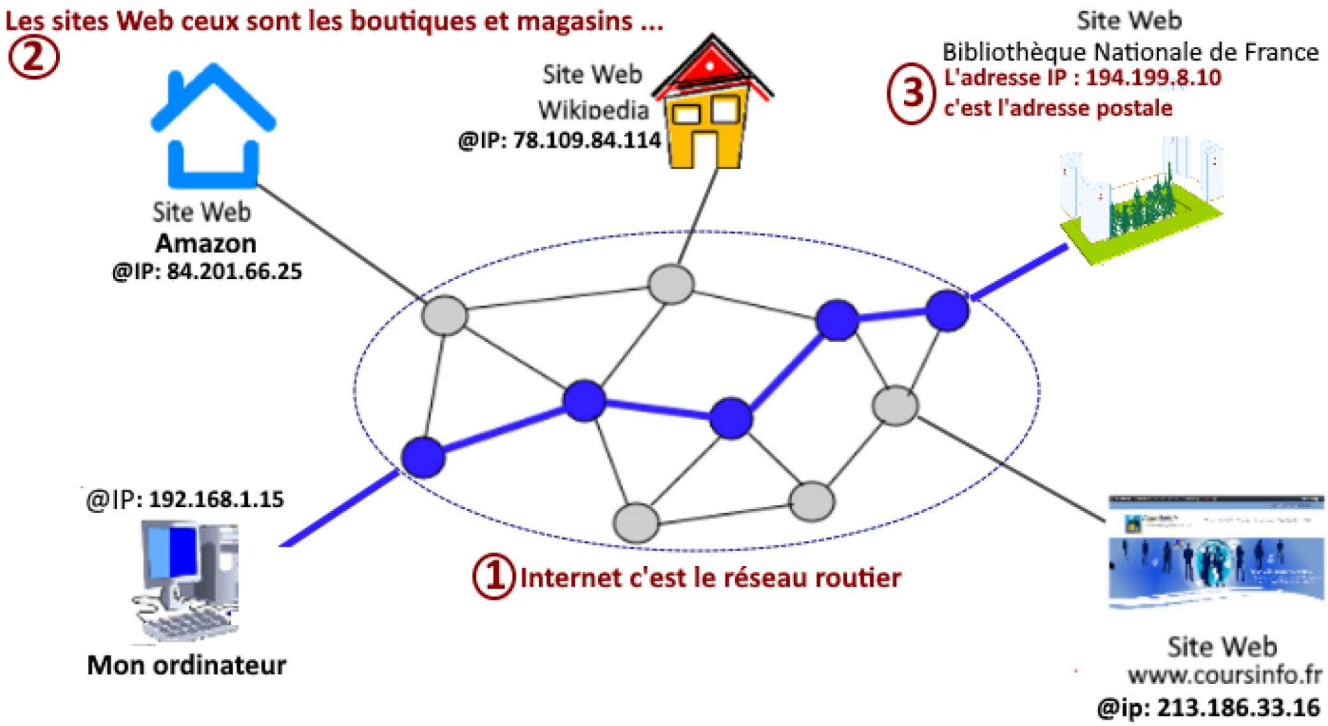


Illustration 5: Illustration de la navigation sur l'internet

Pour se rendre à la **Bibliothèque Nationale de France**, on se **déplace** par Internet à l'**adresse IP** : 194.199.8.10

*Nota :Si la machine fait partie d'un réseau local (par exemple votre maison), son adresse IP sera interne à ce réseau ; pour communiquer à l'extérieur de ce réseau (Internet), la machine sera identifiée par une **adresse IP publique**.*

Exercices :

La « box » internet n'est pas représentée sur le schéma ci-dessus. Où se situe t'elle ?
Questions plus difficiles... : De qu'elle type serait son adresse IP ? A t'elle plusieurs adresses ?

Qu'est-ce qu'un nom de domaine? c'est l'équivalent de l'adresse IP

Chaque **ordinateur** directement connecté à internet possède une **adresse IP**. Pour se connecter à l'un d'eux, il est compliqué de retenir et manipuler un ensemble de chiffres (adresse IP).Le but d'un **nom de domaine** est de **retenir et communiquer facilement l'adresse d'un site Web**.

Par exemple, le **nom de domaine** : « **coursinfo.fr** » est plus simple à mémoriser que **213.186.33.16.**

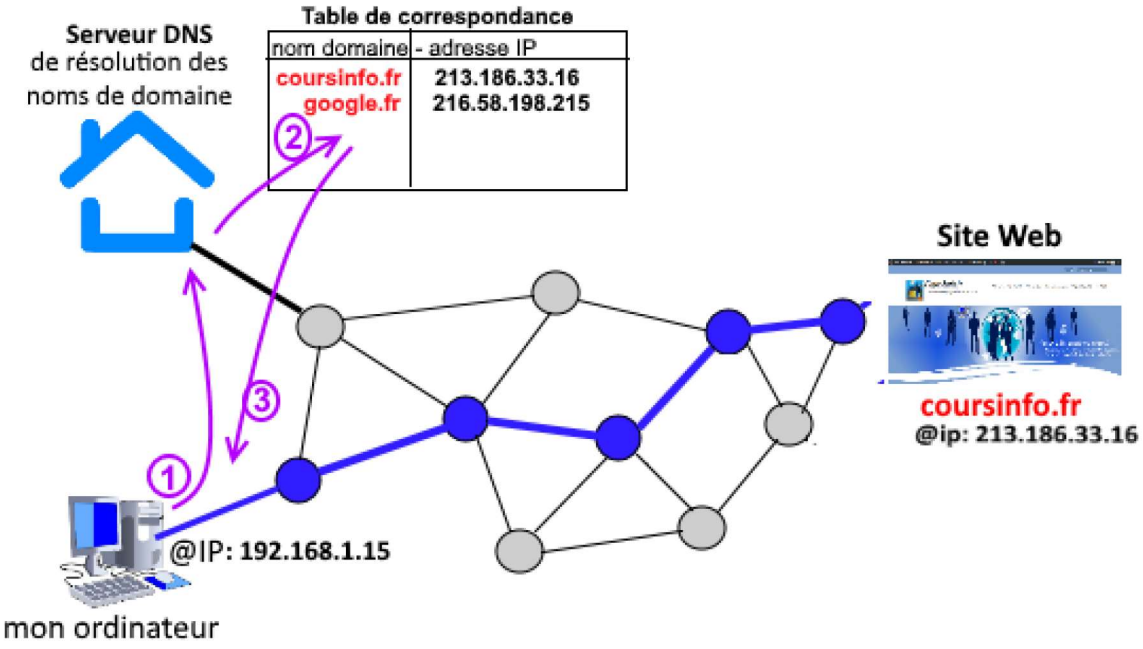


Illustration 6: Usage du DNS

Le rôle du **serveur DNS** (*Domain Name System*) est tout simplement **d'associer un nom de domaine à une adresse IP**, un peu comme la ferait un **annuaire téléphonique** avec les **numéros de téléphone et les noms des usagers**.

Dans cet exemple, je veux me connecter au site web coursinfo.fr :

1. mon ordinateur demande au **serveur DNS** : quelle est l'**adresse IP** correspondant au nom de domaine **coursinfo.fr**

2. le serveur DNS recherche dans se table de correspondance quelle est l'**adresse IP associée**

3. le serveur DNS répond à mon ordinateur que l'adresse IP est : **213.186.33.16**

Qu'est-ce qu'une url ?

L'**URL** *(Uniform Ressource Locator)* est l'**adresse unique** qui permet d'accéder à **une page web** à partir de sa saisie dans la **barre d'adresses du navigateur**. L'**URL** est communément appelée : l'**adresse web** d'une page.

L'**URL** d'une page de cours est par exemple :
« http://www.coursinfo.fr/decouverte/internet/quest-quune-adresse-ip-nom-de-domaine/»
Prenons l'exemple : http://www.coursinfo.fr/ cette **URL** se compose de **4 blocs** :

- **Http://** qui désigne le protocole à utiliser pour accèder au site web : ici c'est donc le **protocole http**

- **www** le **www** est la **norme pour les sites Web** (*World Wide Web*)

- **coursinfo** désigne le **nom de domaine** du site web – le site coursinfo.fr a souscrit à ce nom de domaine

- .fr désigne l'**extension** du nom de domaine

> *Pour vous simplifier la saisie, les navigateurs ajoutent automatiquement le **http://.** Il est donc inutile de le taper puisque le navigateur l'ajoutera pour vous.*

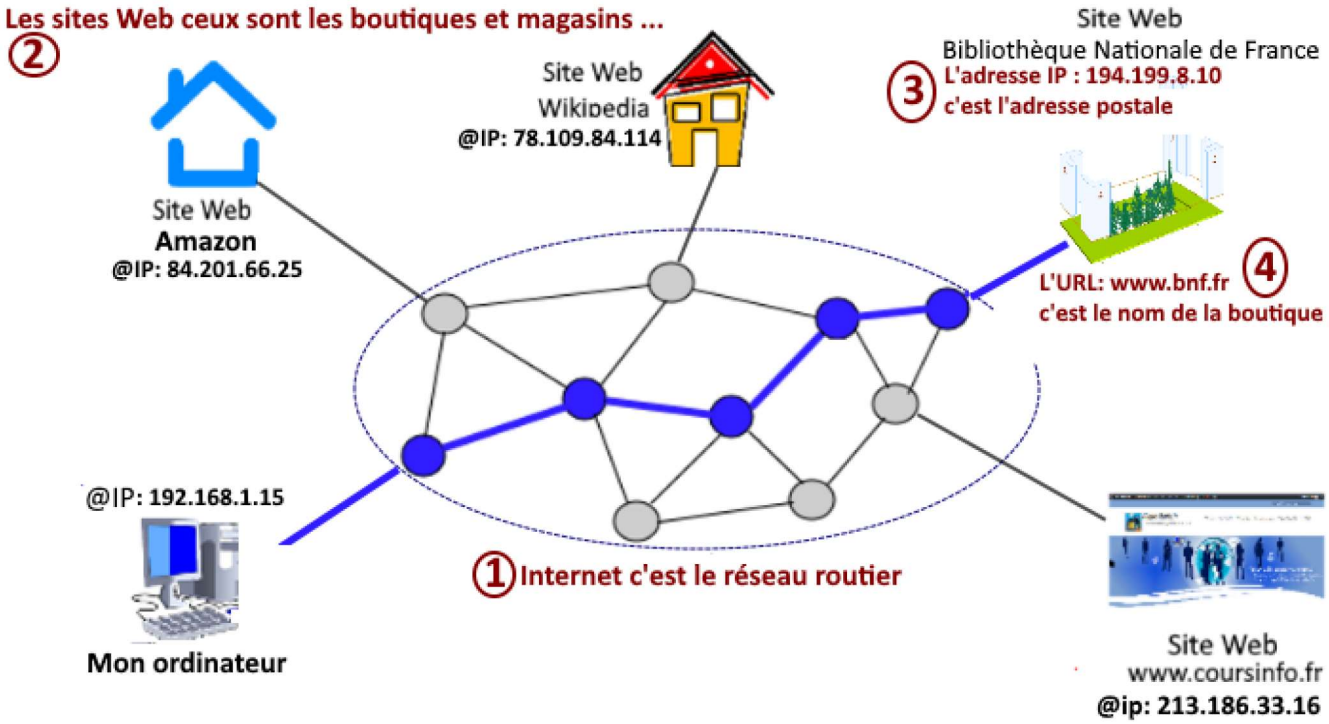


Illustration 7: En route vers L'URL www.bnf.fr

L'URL ***www.bnf.fr*** *c'est le* ***nom de la boutique Bibliothèque Nationale de France*** *sur Internet.*

Travaux pratiques

Exercice 1: tester l'hypertexte en utilisant un navigateur et un moteur de recherche.

Exercice 2 : tester un service de streaming tel que Molotov et un service de replay TV. Répondre à la question : est-ce que ces services sont des services web ?

Autres exercices :

http://www.coursinfo.fr/decouverte/internet/travaux-pratiques-sur-internet/

2.1.2 Notions complémentaires sur "le web"

2.1.2.1 C'est quoi un navigateur ?

Un **navigateur** est un outil permettant de **naviguer** et de **consulter** les pages web disponibles sur les **sites web**. En pratique, le **navigateur nous traduit en texte et image** les pages d'information qui sont **codées** en **HTML**.

En pratique, le **navigateur** c'est l'équivalent de votre **voiture** pour vous **déplacer sur le réseau routier Internet** !

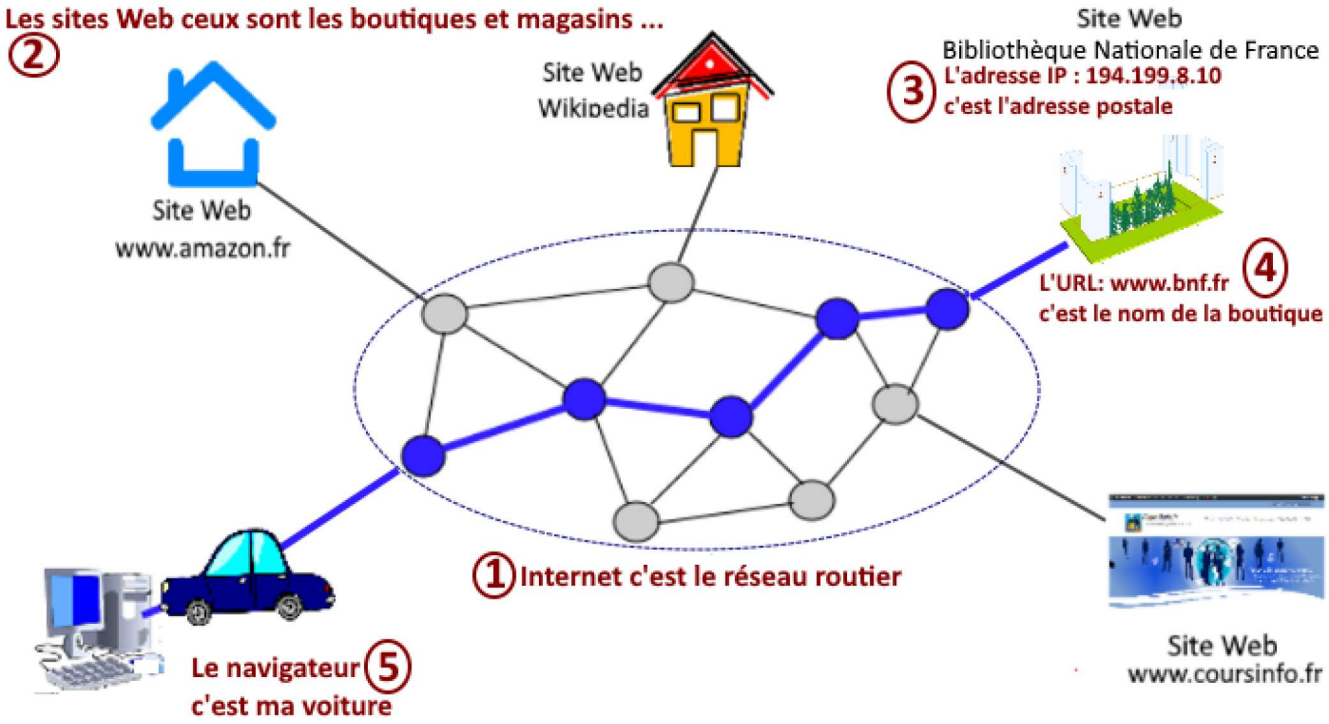


Illustration 8: La navigation sur internet

*"Pour visiter le site www.coursinfo.fr ou www.bnf.fr, vous utilisez un **navigateur** qui vous permet de vous déplacer sur le réseau routier Internet afin d'y aller.*

Il existe de nombreux navigateurs Web, mais les plus populaires sont : **Firefox** de Mozzila, **Edge** de Microsoft (le remplaçant d'Internet Explorer), **Google Chrome** et **Safari** d'Apple. Ils sont tous **gratuits**.

2.1.2.2 Pourquoi utilise t'on le «HTTP ou le HTTPS pour se connecter sur un site ?

Lorsque l'on se se connecter à un site internet, le navigateur choisit d'utiliser soit le protocole HTTP :

par exemple: http://www.coursinfo.fr

ou, le protocole HTTPS

par exemple: https://www.impots.gouv.fr/portail

Le « S » du HTTPS signifie « Sécurisé ».

Ce qu'il faut retenir donc :

- Les sites HTTP sont non sécurisés et les données passent en clair sur le réseau « routier » internet.
- Les sites HTTPS sont dit sécurisés et les données sont chiffrées. De plus, l'identité du site est validé pour éviter des usurpations.

Le HTTPS et son principe de fonctionnement est détaillé au chapitre : Application du chiffrement dans le web.

2.1.2.3 C'est quoi un client Web, un serveur Web?

Un client Web est un logiciel installé dans une machine : PC, smartphone, enceinte connecté par exemple. Lorsque vous entrez le nom d'un serveur web ou vous posez une question à une enceinte connectée, le client web se connecte à un serveur web pour recevoir ou lui envoyer des informations.

Par exemple, le navigateur google chrome ou firefox est client web.

Une application sur votre smartphone qui interroge un site web est aussi un client web : par exemple, gmail se connecte au site web de google pour envoyer ou recevoir vos messages.

La figure ci-dessous illustre comment les clients et serveurs communiquent sur l'internet.

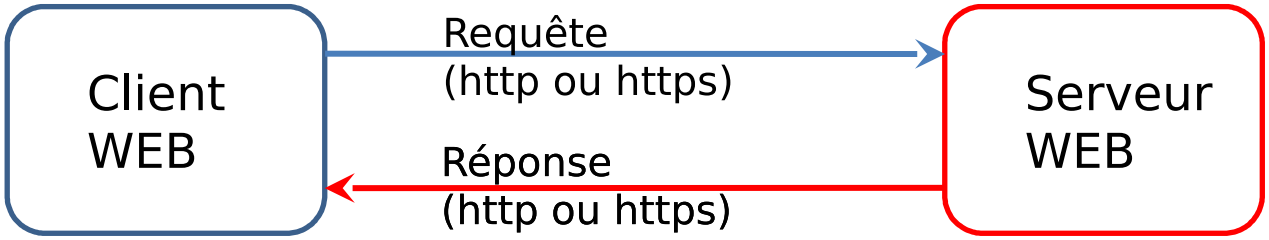


Illustration 9: Échanges entre client et serveur

Un serveur web se comporte en client Web lorsqu'il fait une requête vers un autre site Web.

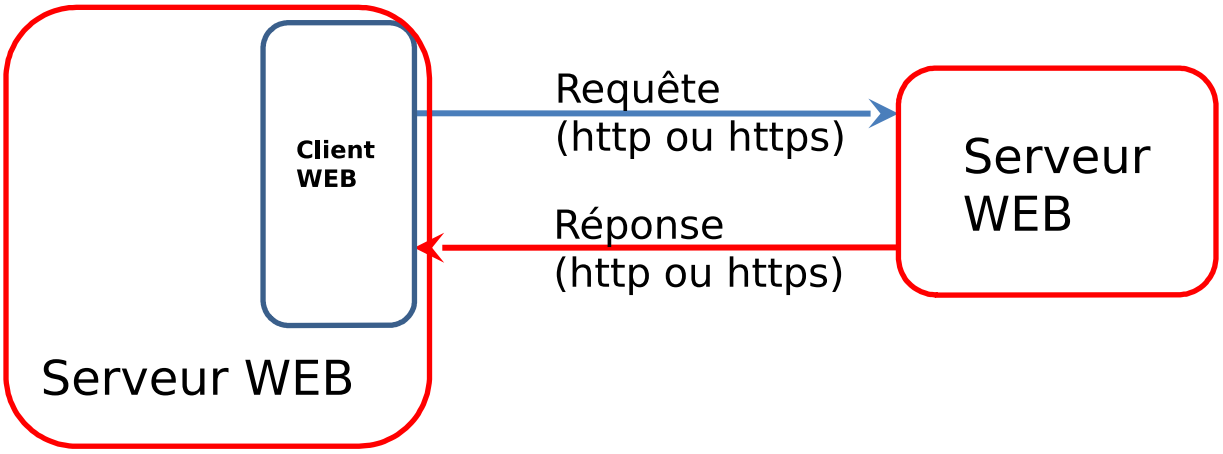


Illustration 10: Échanges entre serveur web à l'aide d'un client web

2.1.2.4 Comment fonctionne un serveur web ?

Un serveur lance un ou plusieurs programme simultanément pour répondre à plusieurs clients à la fois.

On peut imaginer un serveur web comme un logiciel qui écoute pour recevoir des requêtes et renvoi des réponses associées à ces requêtes en « simultanéité » (apparente).

La figure ci-dessous illustre ce fonctionnement.

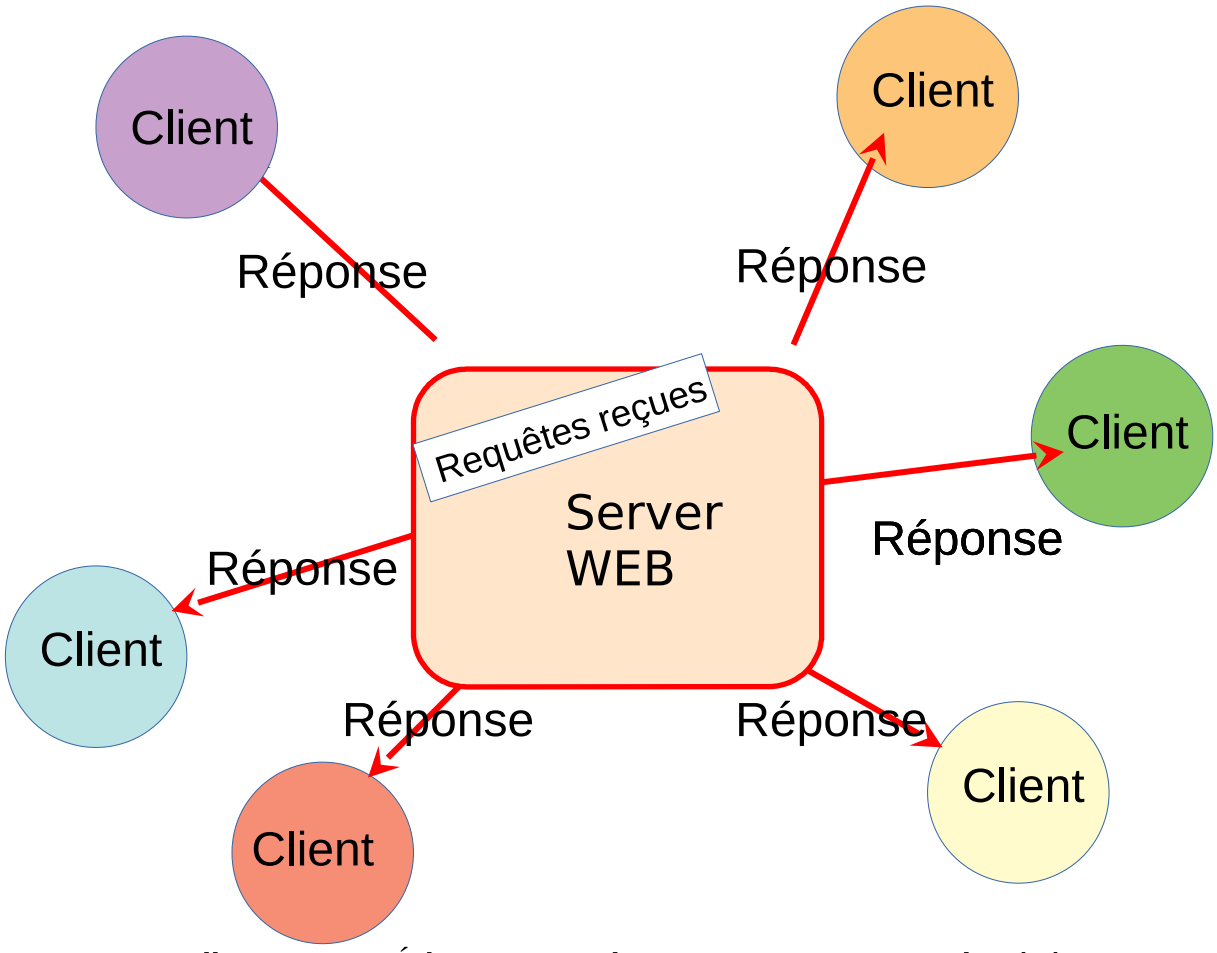


Illustration 11: Échanges entre clients et un serveur en simultanéité

2.1.2.5 C'est quoi le « port » d'un serveur web ?

Chaque machine (PC, Smartphone…) dans un réseau est identifiée par une adresse IP par exemple : 10.3.1.141.1. Cette adresse IP est l'équivalent d'un numéro d'immeuble.

Une machine peut héberger plusieurs sites web comme un immeuble peut héberger plusieurs appartements. Le port est l'équivalent d'un numéro d'appartement dans un immeuble.

En général, le port d'un site web est : 80. S'il existe d'autres sites web dans une même machine, on leurs donne en général des numéros de port de type 80xy ou 500x.

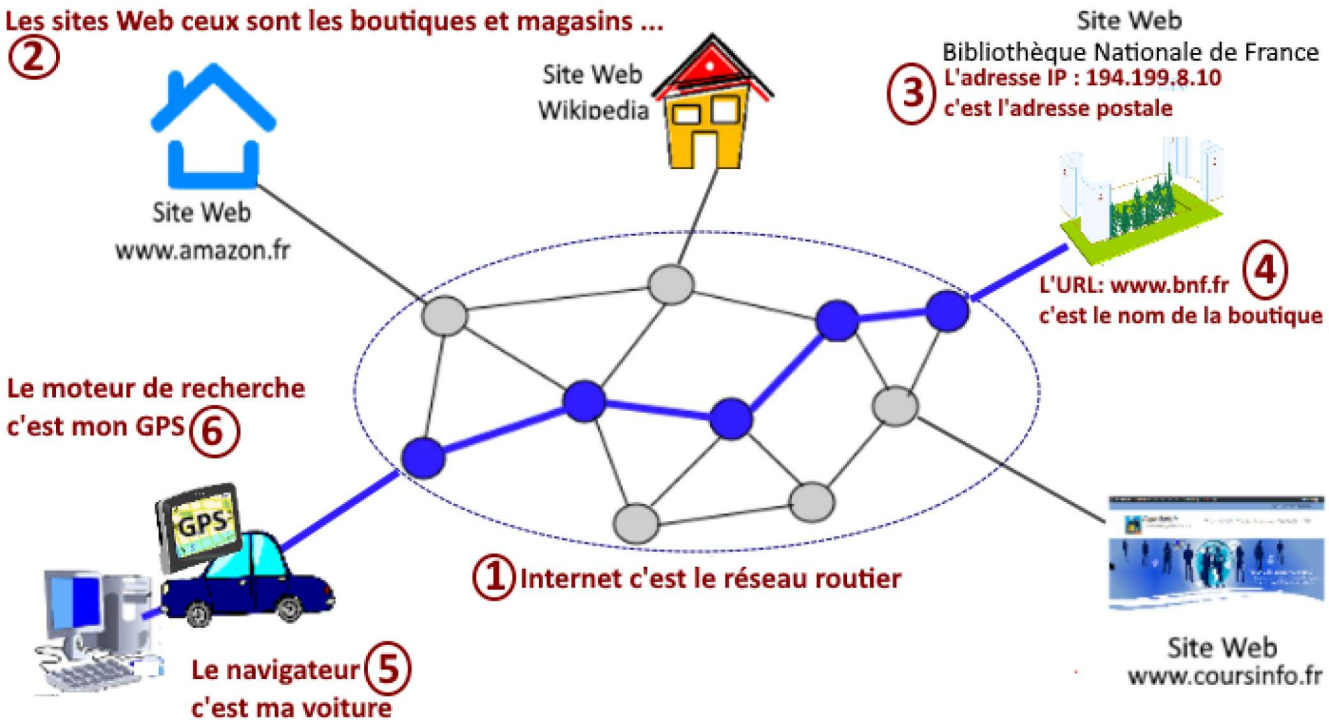
Par exemple la requête http://10.3.141.1:8080/ envoyée depuis un navigateur permet d'accèder à la machine dont l'adresse IP est : 10.3.141.1 et au programme « site web » identifié par le port : 8080.

2.1.2.6 C'est quoi un moteur de recherche ?

Il existe des **milliards de pages** enregistrées sur **des millions de sites Web** répartis sur toute la planète. **Chaque page** contient des **mots clés** décrivant son **contenu**.

Un **moteur de recherche** est un service en ligne permettant de **trouver facilement une de ces pages sur le Web** grâce à un ou plusieurs **mots-clés** renseignés dans un **formulaire de recherche**.

En pratique, **un moteur de recherche c'est un peu votre GPS pour vous déplacer sur le réseau routier Internet**. Il vous guidera dans vos déplacements sur Internet :



*"Vous **programmez** votre **moteur de recherche** comme un **GPS** en lui donnant des **mots clés** décrivant les sites que vous souhaitez visiter !*

Comment marche un Moteur de recherche ?

Un **moteur de recherche** fonctionne grâce à un grand nombre de serveurs appelés **robots qui parcourent les sites Web existants** à intervalle régulier pour **découvrir les liens des milliards de pages** Web. Chaque page identifiée est alors **indexée dans une base de données, accessible** ensuite par les internautes **à partir de mots-clés**.

Lorsqu'un Internaute utlise un **moteur de recherche**,

1. Il saisit les **mots clés** décrivant **les pages qu'il recherche,** par exemple **: cours informatique gratuit et sans pub**
   *soit directement dans la **barre d'adresse et de recherche** soit sur le **site web du moteur de recherche***

2. le navigateur prépare ensuite un **formulaire de recherche** contenant ces **mots-clés** et l'envoie au **moteur de recherche**

3. **Le moteur de recherche interroge sa base de données** pour chacun des **mots-clés** puis **affine la recherche** en enlevant les pages ne convenant pas

4. La base de données répond avec **une liste de résultats contenant les liens** vers les pages adéquates

5. Le **moteur de recherche** retourne au **navigateur cette liste de résultats** contenant **liens vers des pages**, avec soit le **début du texte de la page**, soit le **texte spécifié par le créateur de la page** grâce aux **balises spécifique**s, appelées **méta-tags**, ou encore l'**extrait de la page** qui contient les **mots recherchés**.

6. Le navigateur affiche **la liste de résultats** à l'Internaute.

*Les réponses sont classées dans un **ordre de pertinence**, selon une méthodologie propre à chaque moteur de recherche. Tous essayent d'avoir les résultats les plus pertinents, dans le but d'attirer le plus de visiteurs et d'y vendre plus de publicités..*

Liste des principaux moteurs de recherche

Google :

Google, qui a donné le nom à la **société Google**, est le moteur de recherche sur le Web **le plus utilisé au monde** avec environ **90 % du marché**.

Google se démarque aussi de la concurrence avec des **fonctionnalités supplémentaires** :

- Google Images, pour rechercher des images,

•Google Vidéos, pour rechercher des vidéos,

•Google Maps, pour rechercher un itinéraire ou consulter une carte géographique.

Bing

Bing est un moteur de recherche **développé par Microsoft** et lancé en **2009**. Bing offre des **options de recherches** tels que des **images, vidéos, sites web, actualités, cartes**… Ce moteur de recherche donne des **résultats pertinents**, organisés et **classés en rubriques thématiques**.

Qwant

Le moteur de recherche français repose sur le principe du **respect de la vie privée**. Le moteur s'engage non seulement à **ne pas filtrer le contenu du Web**, mais également à **ne pas tracer ses utilisateurs**.
Qwant ne se fait pas payer par la publicité mais par des **commissions prélevées aux boutiques en ligne** lorsque des internautes y réalisent des achats via sa catégorie Shopping.

2.1.2.7 Bien choisir son fournisseur d'internet

Pour accèder au **réseau Internet**, vous devez disposer d'un **accès Internet**.

Pour celà, vous devez **souscrire à un abonnement** auprès d'un **Fournisseur d'Accès Internet** (appelé *FAI* ou *opérateur*).

En France, les principaux fournisseurs d'accès sont **Orange**, **SFR**, **Bouygues** et **Free**.
Les **prestations** proposées sont :

•l'**accès** au réseau Internet (Haut débit illimité)

•la **télévision** (un bouquet d'une centaine de chaines gratuites disponible via un boitier TV)

•**la téléphonie** (téléphone illimité sur le fixe en France et dans certains pays)

•l'appel depuis un **mobile**

> *On parle d'**offre triplay** pour les 3 prestations : "accès, télévision, téléphonie".*

En fonction de l'endroit où est situé votre logement, le fournisseur proposera de vous raccorder :

•par le **cable** (en haut débit)

•en **ADSL** (en haut débit jusqu'à 20 Gigabits/s si votre zone est dégroupée)

•en **fibre optique** si vous êtes éligible : très haut débit jusqu'à 100 Gigabits/s

Choisissez l'abonnement le plus adapté à **vos besoins et à vos moyens**. Soyez vigilant sur les tarifs et les **différents frais**(*raccordement*, *résiliation*…) qui vous seront prélevés. Enfin, vérifiez la **durée de l'engagement** (6, 12 ou 24 mois) proposé par l'**opérateur**. Comparer les prix en accédant à un site comparateur de prix.

Si vous êtes un nomade ou si vous ne disposez pas d'un **accès Internet fixe** (box), vous pouvez alors souscrire à un forfait Internet mobile.

Votre opérateur vous fournira alors une clé 3G/4G vous permettant d'accèder au **réseau Internet depuis vos terminaux mobiles** : PC portable, tablette ou smartphone.

Vous devrez choisir pour votre forfait un **volume de données**autorisé par mois : 2, 10 ou 20 GigaOctets, ou encore illimité

Si vous disposez d'un abonnement mobile autorisant un volume important de données (data), vous pouvez aussi utiliser votre smartphone comme ***clé 3G/4G****. Dans ce cas, paramétrez votre* ***smartphone****comme un* ***point modem.***

2.1.2.8 Mise en pratique pour démystifier toutes ces notions

présentation d'un serveur web simple , html, CSS en WiFi

expliquer parallélisme dans les machines

expliquer les communications inter-servers

expliquer/montrer des adresses IP locales

voir: http://www.coursinfo.fr/decouverte/internet/comment-naviguer-sur-internet/

2.1.3 Les services de sécurité dans le monde connecté

2.1.3.1 Pourquoi des services de sécurité ?

Les services de sécurité du monde connecté ont pour objectifs

- d'assurer la sûreté de nos échanges,
- et de protéger nos données personnelles.

2.1.3.1.1 Besoin de faire des échanges sûrs

Pour nos démarches de types administratives, financières ou professionnelles que nous faisons sur le monde connecté, nous avons besoin que :

- que les informations échangées puissent être confidentielles,

  En effet, Il est très facile d'enregistrer toutes les informations qui passent sur un réseau si on y est connecté. (en wifi par exemple). C'est pourquoi, il est nécessaire de faire très attention aux données échangées sur les réseaux publics tels que les aéroports, les hôtels, ...
  Et il est également possible d'écouter un réseau sans y être connecté. En effet, en circulant dans les câbles, les informations émettent des ondes qu'il est possible de capter.

- que le site web avec lequel nous communiquons soit bien le vrai site authentique et non un site usurpateur,
- que ces informations ne soient pas modifiées à notre insu durant l'échange.

Pour couvrir ces besoins de **confidentialité**, d'**intégrité** et d'**authentification** , le monde connecté utilise le chiffrement. Voir le chapitre : comprendre les grands principes du chiffrement ci-dessous pour en comprendre l'essentiel.

2.1.3.1.2 Besoin de protéger nos données personnelles hébergés dans les sites web

Lorsque nos données sont hébergés dans des sites web, il est nécessaire qu'elles ne soient pas utilisées sans notre consentement.

Pour protéger ces données et donc notre vie privée, la commission européenne a créé en mai 2018 un Règlement général sur la protection des données (RGPD).

Il contraint les entreprises européenne à apporter la preuve de leur **mise en conformité** au RGPD

En particulier, les sites web européens qui collectent des données personnelles doivent :

- Informer sur la collecte des données :
- Obtenir un consentement explicite :
- Protéger la transmission des données personnelles en utilisant le HTTPS
- Nommer un délégué à la protection des données
- Tenir un registre de traitement des données
- Créer une base interopérable pour le droit à la portabilité

ref: https://fr.wikipedia.org/wiki/Règlement_général_sur_la_protection_des_données

ref : http://www.capsurlenumerique.fr/rgpd-site-internet

Le RGPD s'applique à toutes les entités situées sur le territoire européen .

Le RGPD s'appliquera toujours si les activités du responsable des traitements ont pour cible un citoyen européen et ce même si le responsable du traitement est situé en dehors de l'UE.

Ref : **https://www.dpms.eu/rgpd/rgpd-mondial-europeen/**

2.1.3.2 Comprendre les grands principes de la cryptographie

Ce chapitre est issu de la **CNIL**.

Historiquement, la cryptologie correspond à la science du secret, c'est-à-dire au chiffrement. Aujourd'hui, elle s'est élargie au fait de prouver qui est l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numériques et aux fonctions de hachage.

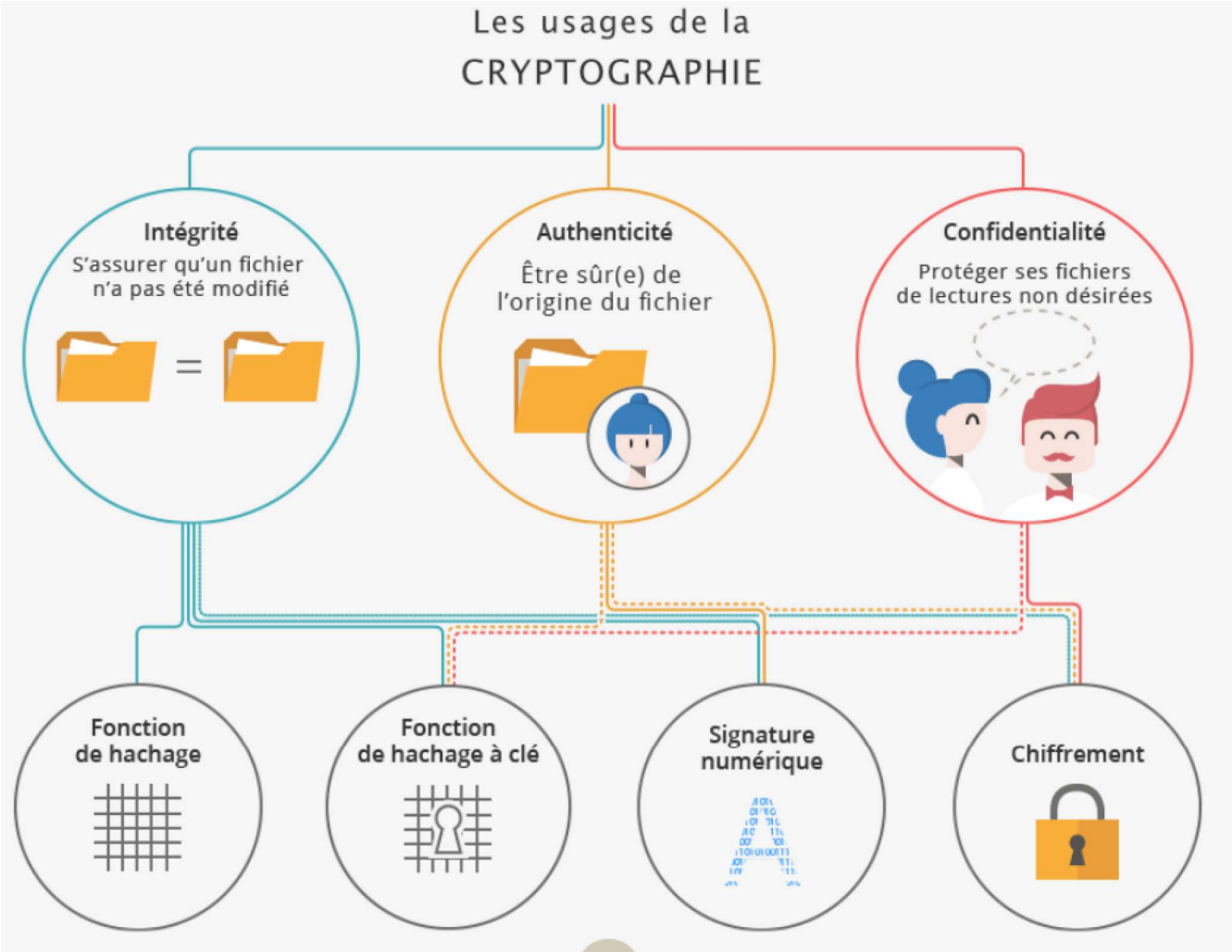


Illustration 12: Relations entre les besoins en sécurité et les solutions techniques en cryptographie

Étymologiquement, la cryptologie est la science (λόγος) du secret (κρυπτός) . Elle réunit la cryptographie (« écriture secrète ») et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie).

La cryptologie ne se limite plus aujourd'hui à assurer la confidentialité des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions : assurer l'authenticité d'un message (qui a envoyé ce message ?) ou encore assurer son intégrité (est-ce qu'il a été modifié ?).

Pour assurer ces usages, la cryptologie regroupe quatre principales fonctions : le hachage avec ou sans clé, la signature numérique et le chiffrement.

Pour expliquer la cryptologie, nous utiliserons dans nos exemples les personnages traditionnels en cryptographie : Alice et Bob.

2.1.3.2.1 Pourquoi la cryptologie existe-t-elle ?

2.1.3.2.1.1 Pour assurer l'intégrité du message : le hachage

La cryptologie permet justement de détecter si le message, ou l'information, a été involontairement modifié. Ainsi, une « **fonction de hachage** » permettra d'associer à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous.

Une fonction de hachage, c'est en fait tout simple. Cela consiste en une fonction qui transforme une donnée quelconque en une donnée de taille fixée.

Cette empreinte est souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l'algorithme utilisé, par exemple « SHA2» ou « SHA256 ».

Exercice : TP hachage, md5sum

Il ne faut pas confondre le chiffrement, qui permet d'assurer la confidentialité, c'est-à-dire que seules les personnes visées peuvent y avoir accès (voir « **Pour assurer la confidentialité du message** »), et le hachage qui permet de garantir que le message est intègre, c'est-à-dire qu'il n'a pas été modifié.

> **Le hachage, pour quoi faire ?**
> Pour sauvegarder vos photos sur votre espace d'hébergement (de type « cloud » par exemple) et vérifier que votre téléchargement s'est bien déroulé ?
> Pour synchroniser vos dossiers et détecter ceux qu'il faut sauvegarder à nouveau et ceux qui n'ont pas été modifiés ?

Il existe aussi des « **fonctions de hachage à clé** » qui permettent de rendre le calcul de l'empreinte différent en fonction de la clé utilisée. Avec celles-ci, pour calculer une empreinte, on utilise une clé secrète. Pour deux clés différentes l'empreinte obtenue sur un même message sera différente. Donc pour qu'Alice et Bob calculent la même empreinte, ils doivent tous les deux utiliser la même clé.

C'est parmi ces fonctions de hachage à clé que l'on trouve celles utilisées pour stocker les mots de passe de façon sécurisée.

Le hachage à clé, pour quoi faire ?

Votre service préféré reconnaît votre mot de passe quand vous vous connectez ?
Vous voulez pouvoir détecter si quelqu'un modifie des documents sans vous le dire ?

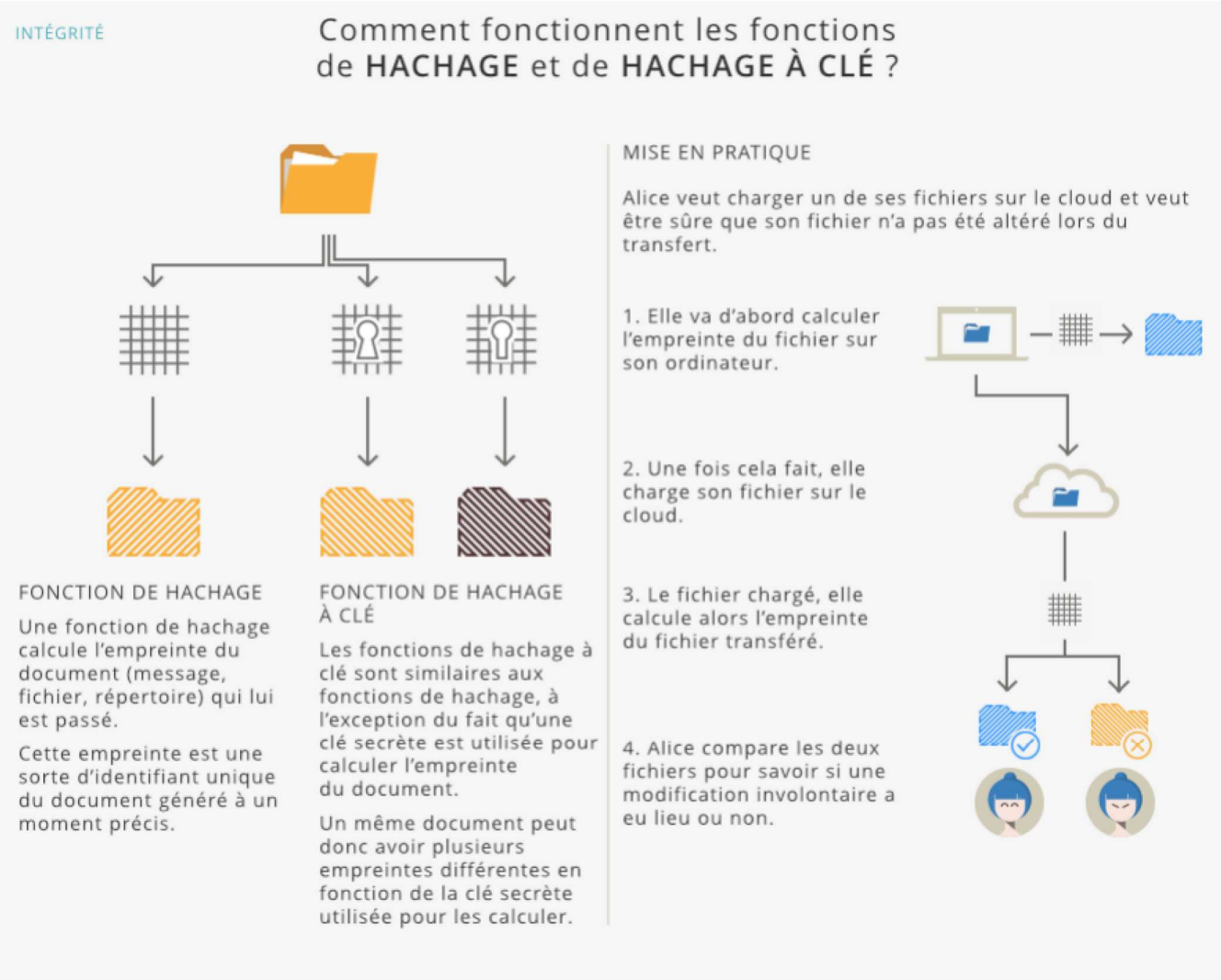


Illustration 13: Le hachage

Bien entendu, la donnée en question peut avoir plusieurs formes. Ce peut être du texte, une image, … mais dans tous les cas la donnée sera transformée en un texte binaire avant qu'on lui applique la fonction de hachage.

2.1.3.2.1.2 Pour assurer l'authenticité du message : la signature

Au même titre que pour un document administratif ou un contrat sur support papier, le mécanisme de la « **signature** » - numérique - permet de vérifier qu'un message a bien été envoyé par le détenteur d'une « clé publique ». Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

La signature numérique, pour quoi faire ?
Vous voulez garantir être l'émetteur d'un courriel ?
Vous voulez vous assurer qu'une information provient d'une source sûre ?

Pour pouvoir signer, Alice doit se munir d'une paire de clés :

- l'une, dite « publique », qui peut être accessible à tous et en particulier à Bob qui est le destinataire des messages qu'envoie Alice ;
- l'autre, dite « privée », qui ne doit être connue que d'Alice.

En pratique, Alice génère sa signature avec sa clé privée qui n'est connue que d'elle. N'importe quelle personne ayant accès à la clé publique d'Alice, dont Bob, peut vérifier la signature sans échanger de secret.

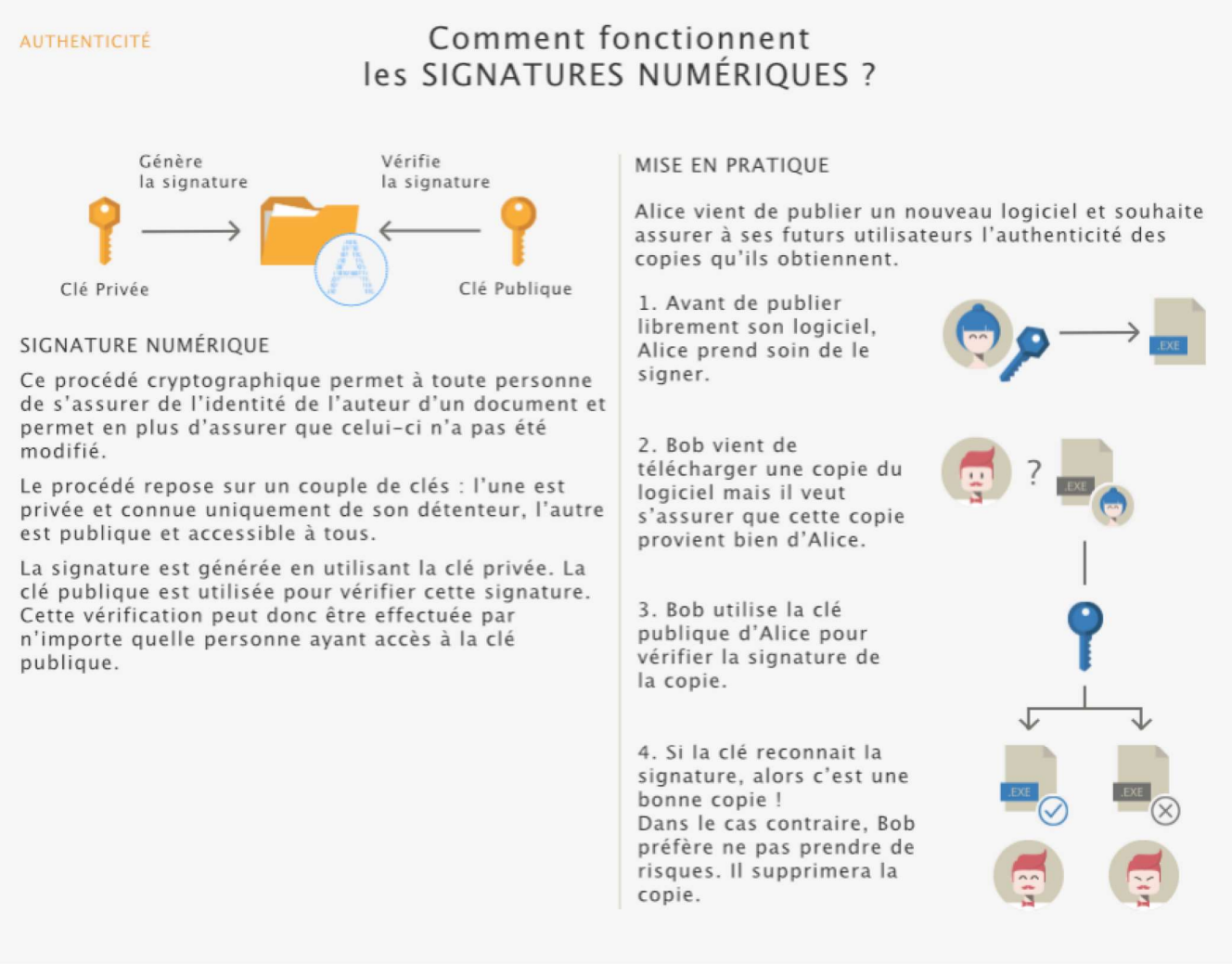


Illustration 14: La signature

2.1.3.2.1.3 Pour assurer la confidentialité du message : le chiffrement

Le chiffrement d'un message permet justement de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu. C'est une sorte d'enveloppe scellée numérique. Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.

Le chiffrement, pour quoi faire ?

Vous voulez vous assurer que seul le destinataire ait accès au message ?
Vous souhaitez envoyer ces informations sous enveloppe numérique et non lisible par tous comme sur une carte postale ?

Il existe deux grandes familles de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.

Le **chiffrement symétrique** permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « clé secrète ». Le chiffrement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit être choisi avec précautions, sans quoi la clé pourrait être récupérée par les mauvaises personnes, ce qui n'assurerait plus la confidentialité du message.

Le **chiffrement asymétrique** suppose que le (futur) destinataire est muni d'une paire de clés (clé privée, clé publique) et qu'il a fait en sorte que les émetteurs potentiels aient accès à sa clé publique. Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer.

Parmi ses avantages, la clé publique peut être connue de tous et publiée. Mais attention : il est nécessaire que les émetteurs aient confiance en l'origine de la clé publique, qu'ils soient sûrs qu'il s'agit bien de celle du destinataire.

Autre point fort : plus besoin de partager une même clé secrète ! Le chiffrement asymétrique permet de s'en dispenser. Mais il est malheureusement plus lent.

Pour cette dernière raison, il existe une technique combinant chiffrements « symétrique » et « asymétrique », mieux connue sous le nom de « chiffrement hybride ».

Cette fois, une clé secrète est déterminée par une des deux parties souhaitant communiquer et celle-ci est envoyée chiffrée par un chiffrement asymétrique. Une fois connue des deux parties, celles-ci communiquent en chiffrant symétriquement leurs échanges. Cette technique est notamment appliquée lorsque vous visitez un site dont l'adresse débute par « https ».

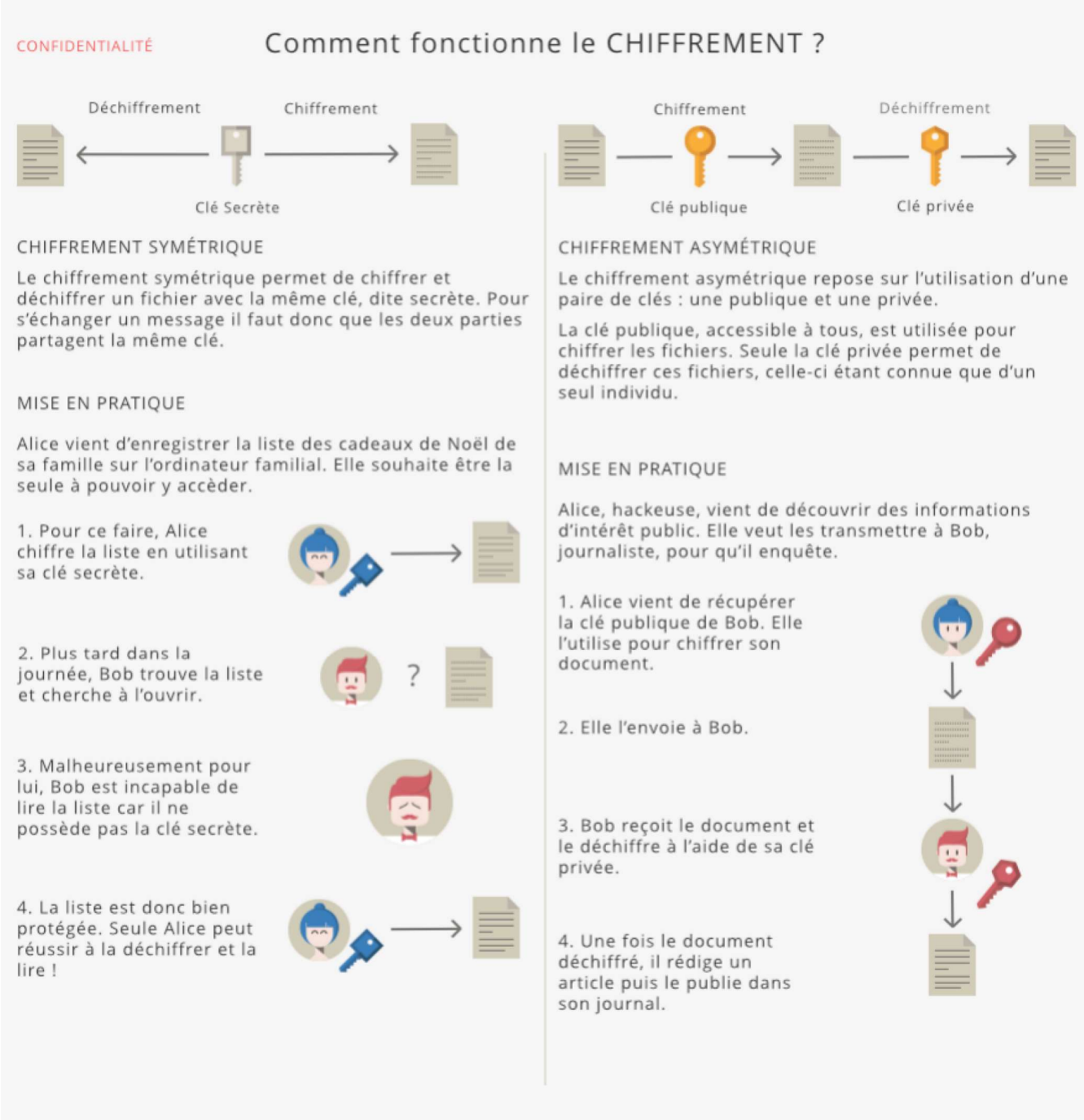


Illustration 15: Le chiffrement

2.1.3.3 Travaux Pratiques et Documents complémentaires

2.1.3.3.1 TP Hachage :

https://cryptage.online-convert.com/fr/generateur-sha256

https://www.cryptage.org/outil-crypto-hachage.html

https://doc.ubuntu-fr.org/md5sum

https://www.it-connect.fr/calculer-une-empreinte-sha1-sous-linux/

2.1.3.3.2 TP chiffrement :

https://www.hostinger.fr/tutoriels/generer-cle-ssh/

http://f4b1.com/securite/comment-creer-une-cle-ssh-publique-et-prive-sous-windows

2.1.3.3.3 Document pour projet éventuel :

https://www.lesinrocks.com/2018/01/03/actualite/actualite/haven-lapplication-anti-espion-dedward-snowden/

2.1.3.3.4 Documents complémentaires :

Synthèse des outils de chiffrement :

https://youtu.be/7W7WPMX7arI

https://www.dpms.eu/rgpd/rgpd-mondial-europeen/

https://www.certeurope.fr/blog/5-choses-a-savoir-au-sujet-des-autorites-de-certification/

2.1.3.4 Application du chiffrement dans le web

2.1.3.4.1 le HTTPS

La figure ci-après présente les différences d'échanges entre le navigateur et le site web selon qu'il choisit d'utiliser le HTTP ou le HTTPS

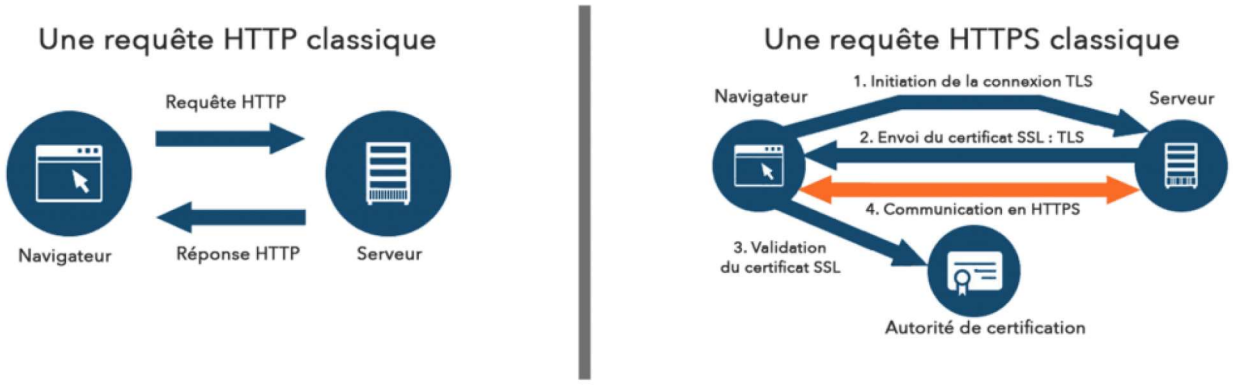
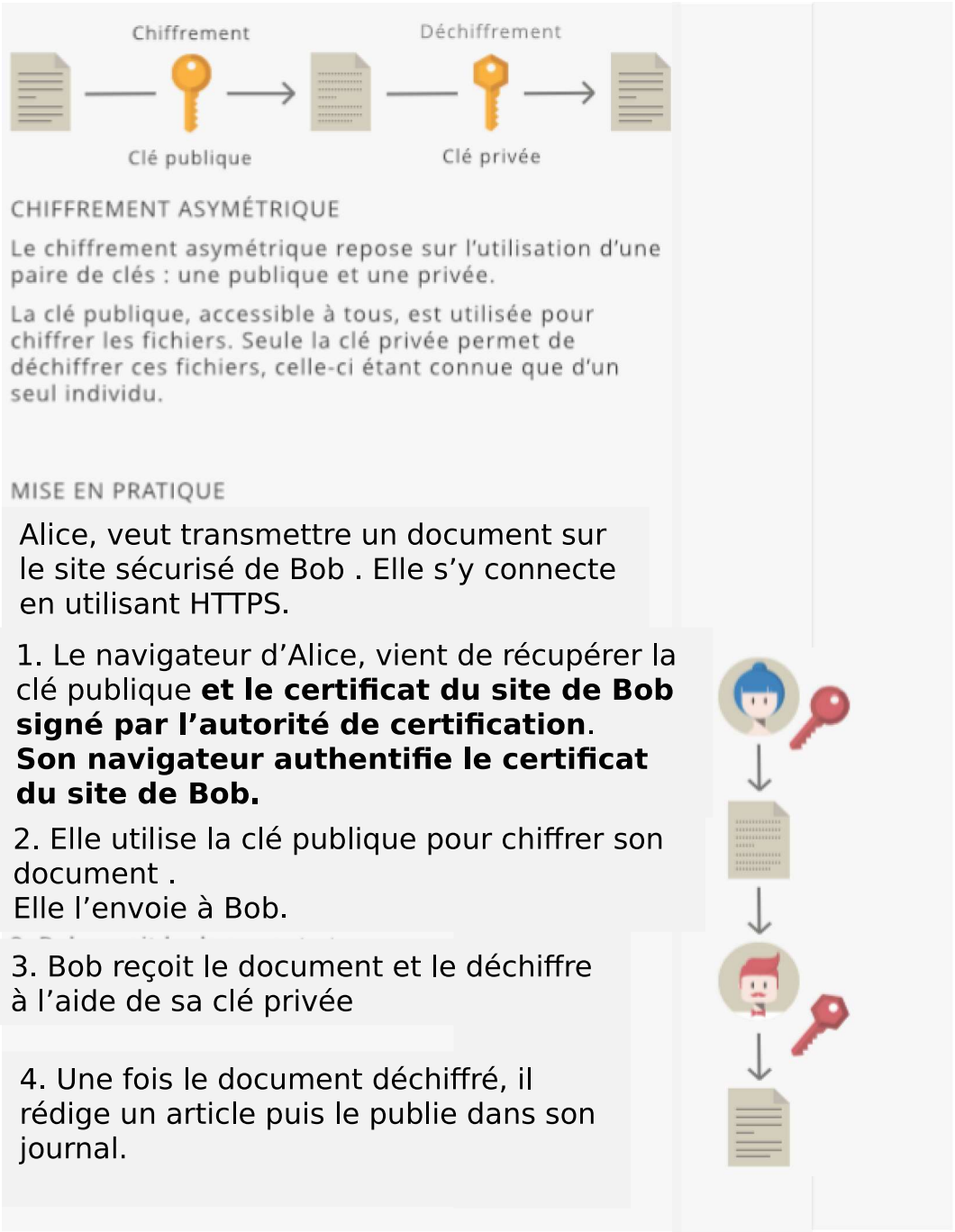


Illustration 16: Schéma d'une requête HTTP vs HTTPS – Source Fasterize

L'échange en HTTPS s'effectue par l'utilisation du chiffrement asymétrique présenté au chapitre précédent. La particularité ajoutée à cette échange est que le navigateur vérifie l'identité du site web. Le serveur envoi son certificat , c'est à dire l'équivalent d'une carte d'identité. Celui-ci est un document signée numériquement par une autorité de certification et renouvelé périodiquement.

La figure ci-après présente comment fonctionne le chiffrement dans un échange HTTPS.



Nota : lors de l'étape 1, le système passe en chiffrement symétrique car le chiffrement asymétrique est plus lent. Voir ici.

2.1.3.5 Applications du chiffrement dans l'internet :

2.1.3.5.1 Le VPN

2.1.3.5.1.1 C'est quoi un VPN ?

Voir video you tube : https://youtu.be/8gYC2DaBDx4.

Celle-ci présente : ce qu'est un VPN, à quoi ça sert et un exemple d'installation et d'utilisation.

La figure ci-dessous illustre ce qu'est **le fonctionnement simplifié d'un Virtual Private Network (VPN).**

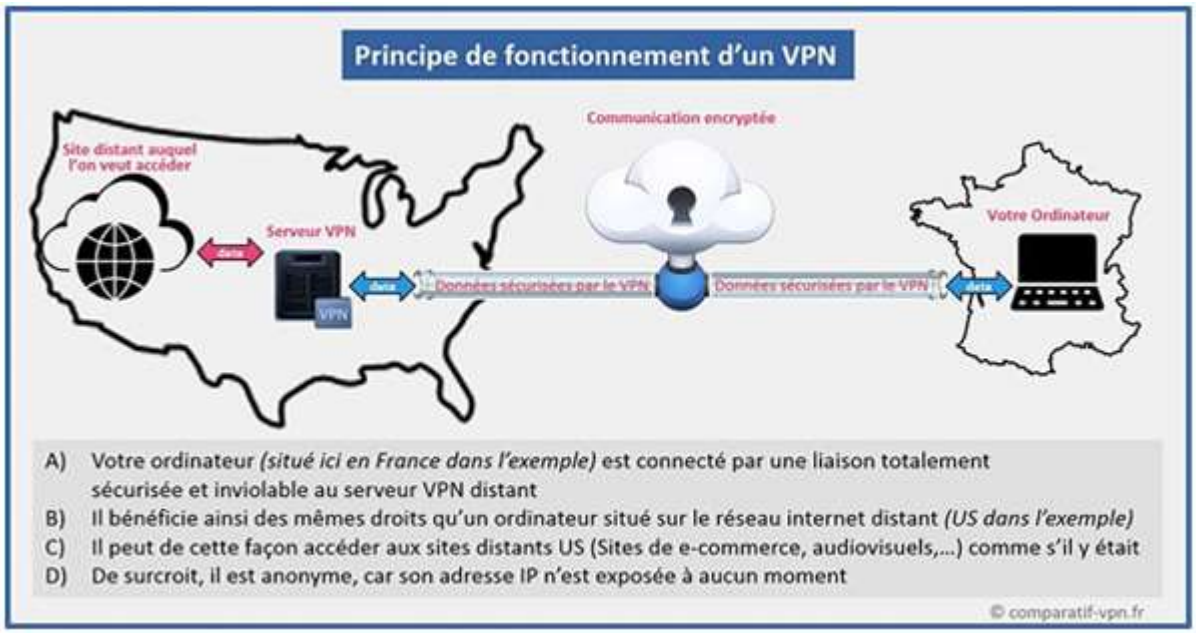


Illustration 17: Principe de fonctionnement d'un VPN

Source: https://comparatif-vpn.fr/definition/

Tout d'abord, il faut savoir que VPN est l'abréviation anglaise de « *Virtual Private Network* ». Traduit en français, on obtient donc « Réseau Privé Virtuel ».

En temps normal, quand vous surfez sur internet, vous êtes sur ce qu'on appelle un « réseau commun ». Autrement dit, **vous y laissez des informations**, qui peuvent être interceptées d'une manière ou d'une autre, notamment par votre fournisseur d'accès internet, par les gouvernements ou par des hackers.

On choisit ainsi un **VPN lorsque l'on cherche à gagner en anonymat sur internet** (ne pensez pas forcément aux mauvaises raisons), en ne laissant ainsi aucune trace de la

navigation grâce à l'absence totale de conservation des logs des meilleurs fournisseurs du marché.

L'utilisateur qui va se connecter sur internet avec un Réseau Privé Virtuel pourra donc facilement crypter ses données.

2.1.3.5.1.2 Se protéger avec un VPN

Le VPN a plusieurs utilisations. Nous pouvons synthétiser ses fonctions en plusieurs points qui sont les suivants :

- **Anonymat** : le VPN vous rend anonyme sur internet en vous donnant une autre adresse IP.
- **Sécurité** : il vous protège sur internet en cryptant vos données avec un protocole AES 256 bits.
- **Streaming** : il vous permet de « streamer » tout et sans limite (Netflix FR, Canal+, TF1, … depuis l'étranger).
- **Téléchargement** : il vous permet de télécharger des torrents en P2P sans risque (parfaite protection face à HADOPI)
- **Censure** : il permet de contourner la censure géographique (Facebook, Whatsapp, Youtube,…en Chine par exemple).
- **Liberté** : il vous permet d'accéder à tous les sites sur internet (casinos, paris sportifs, …).

Exercice :

Mettre en place un VPN gratuit avec le navigateur opera

https://youtu.be/HObc-lXrQqA

Vérifier ma position géographique

https://www.iplocation.net/find-ip-address

2.1.3.5.1.3 Les limites du VPN

Ref : supinfo.com

Malgré de nombreux avantages, les VPN possèdent aussi des inconvénients. En effet, pour avoir un VPN de qualité, il faut très souvent payer celui-ci. Les VPN gratuits ne sont conseillés que pour une utilisation secondaire car ils ont de très nombreux points faibles : une bande passante souvent limitée, un temps de connexion limité, des protocoles VPN peu fiables, des taux de chiffrement très bas, très peu de serveurs VPN disponibles (d'où la réduction de la bande passante), un support client peu professionnel, des coupures fréquentes de la connexion (dues au nombre peu élevé de serveurs disponibles).

Les VPN de qualité sont conseillés pour une utilisation principale mais attention, ils ont aussi leurs limites. En effet, s'ils chiffrent vos données entre votre ordinateur et les VPN, les données sont déchiffrées sur le serveur du fournisseur du VPN, donc lorsque vous en utilisez un, vous offrez une confiance aveugle au fournisseur de ce VPN, car rien ne l'empêche de conserver vos données et de vous espionner.

Un VPN, même de qualité, n'est donc pas nécessairement une garantie pour protéger votre vie privée, il a des avantages pour cela, mais ne vous rend pas anonyme pour autant.

2.1.3.5.2 Les darknets

La techniques de chiffrement est la technique de base utilisée dans les darknets.

Un darknet (que l'on pourrait traduire en français mot pour mot par « internet obscur »), est un réseau superposé à l'internet. C'est-à-dire un réseau bâti sur le réseau internet.

En des termes plus simples, on pourrait définir un darknet comme étant un autre Internet parallèle à celui que nous connaissons (appelé par opposition Clearnet, « l'internet clair »), il est invisible car son fonctionnement est différent. Il est protégé par différentes fonctions d'anonymisation.

Certains comparent un darknet à une zone de non-droit où en échange de monnaie dématérialisée (Bitcoins) il est possible de se procurer différentes choses illégales : codes d'accès à des sites payants, des stupéfiants, des faux billets, des documents contrefaits… Mais cela peut aller encore plus loin : obtenir des numéros de cartes bancaires, de l'armement, des contenus choquants et illégaux, des offres liées au trafic d'êtres humains ou à la disparition de personnes.

Comme vous pouvez le voir, il semble s'y passer des choses assez sombres. Certains de ces sites sont tout de même suspectés d'être des canulars, des arnaques ou d'être élaborés pour arrêter des personnes qui ont recours à des services ou à des produits illégaux. Il existerait aussi des pages consacrées à d'autres thèmes assez délicats.

Mais un darknet ne se limite pas qu'à cela. Il est également utilisé par des ONG, des journalistes et des activistes de certains pays où il y a de la censure et des atteintes à la liberté d'expression. Ils s'en servent pour communiquer ou dénoncer de façon anonyme

2.1.3.5.2.1 Le plus connu des darknets est le réseau Tor.

Source : Les echos

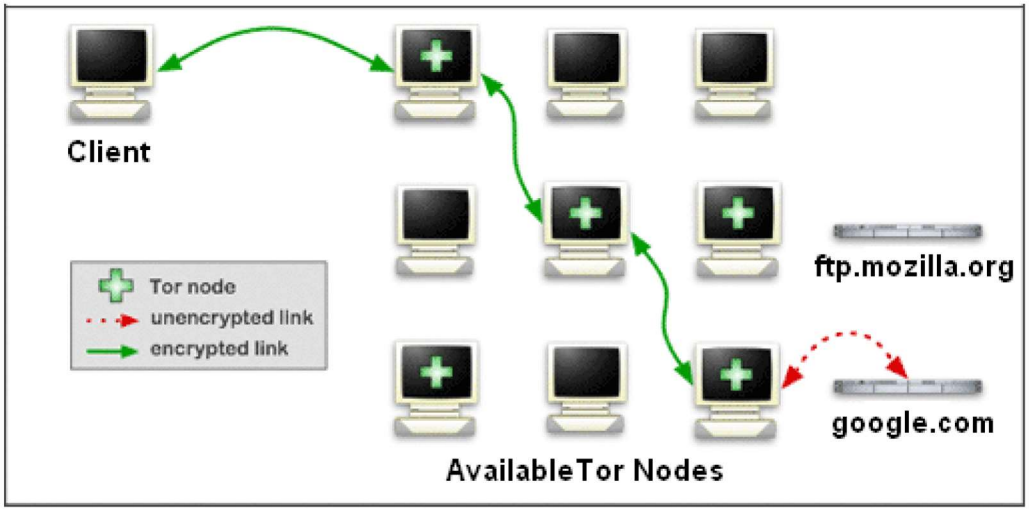
Créé aux USA dans les années 1990 par le US Naval Research Laboratory, Tor a évolué dans un contexte militaire avant de passer sous licence libre en 2004. Depuis 2006, c'est le projet open source " The Tor Project " qui en assure la maintenance, financé à hauteur de 3 millions de dollars .

Les liens suivantes en font une bonne présentation générale : la protection par tor, documentaire tor, Darknet wikipedia , le champion de la surveillance de masse .

2.1.3.5.2.2 Tor: principe de fonctionnement

Source ***: Tor: fonctionnement***

Tor est composé de **multiples relais réseau qui se connectent les uns aux autres**. En utilisant Tor, le trafic réseau s'écoule à travers ces nœuds **utilisant un chemin aléatoire, tout en étant chiffré et déchiffré à la volée**, avant d'atteindre un "nœud de sortie" qui se connectera au service désiré, utilisant une connexion standard.



Exemple of a nodes path

2.1.3.5.2.3 Protéger sa vie privée avec Tor et son smartphone Androïd

Voir au liens : https://www.lesinrocks.com/2018/01/03/actualite/actualite/haven-lapplication-anti-espion-dedward-snowden/ , comment utiliser Tor et l'application Haven sous Android pour surveiller votre domicile. L'application Haven a été lancée par l'ex-consultant de la NSA Edouard Snowden.

D'autres darknets existent, citons : Freenet ,I2p ,GNUnet

2.1.3.5.3 La Blockchain

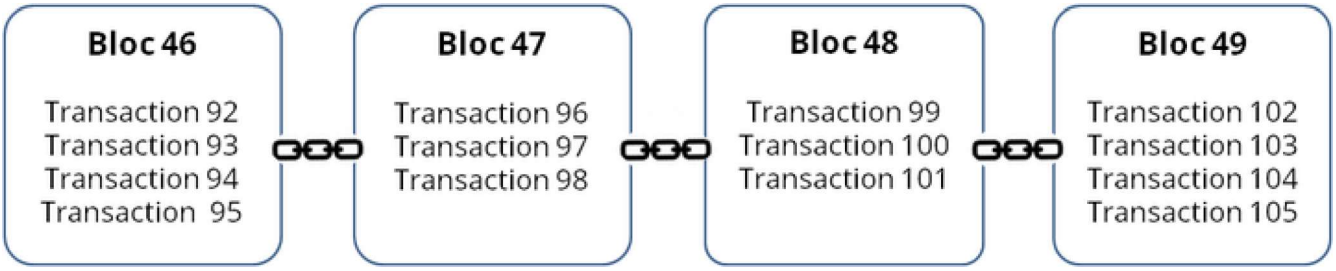
Source : **https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/**

2.1.3.5.3.1 Qu'est-ce que la blockchain ?

Définition et explication

La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle (*définition de Blockchain France*).

Par extension, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne.



Il existe des blockchains publiques, ouvertes à tous, et des blockchains privées, dont l'accès et l'utilisation sont limitées à un certain nombre d'acteurs.

Une blockchain publique peut donc être assimilée à un grand livre comptable public, anonyme et infalsifiable. Comme l'écrit le mathématicien Jean-Paul Delahaye, il faut s'imaginer « un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible. »

2.1.3.5.3.2 Situer la blockchain

La première blockchain est apparue en 2008 avec la monnaie numérique bitcoin, développée par un inconnu se présentant sous le pseudonyme Satoshi Nakamoto. Elle en est l'architecture sous-jacente.

Si blockchain et bitcoin ont été construits ensemble, aujourd'hui de nombreux acteurs (entreprises, gouvernements, etc) envisagent l'utilisation de la technologie blockchain pour d'autres cas que la monnaie numérique.

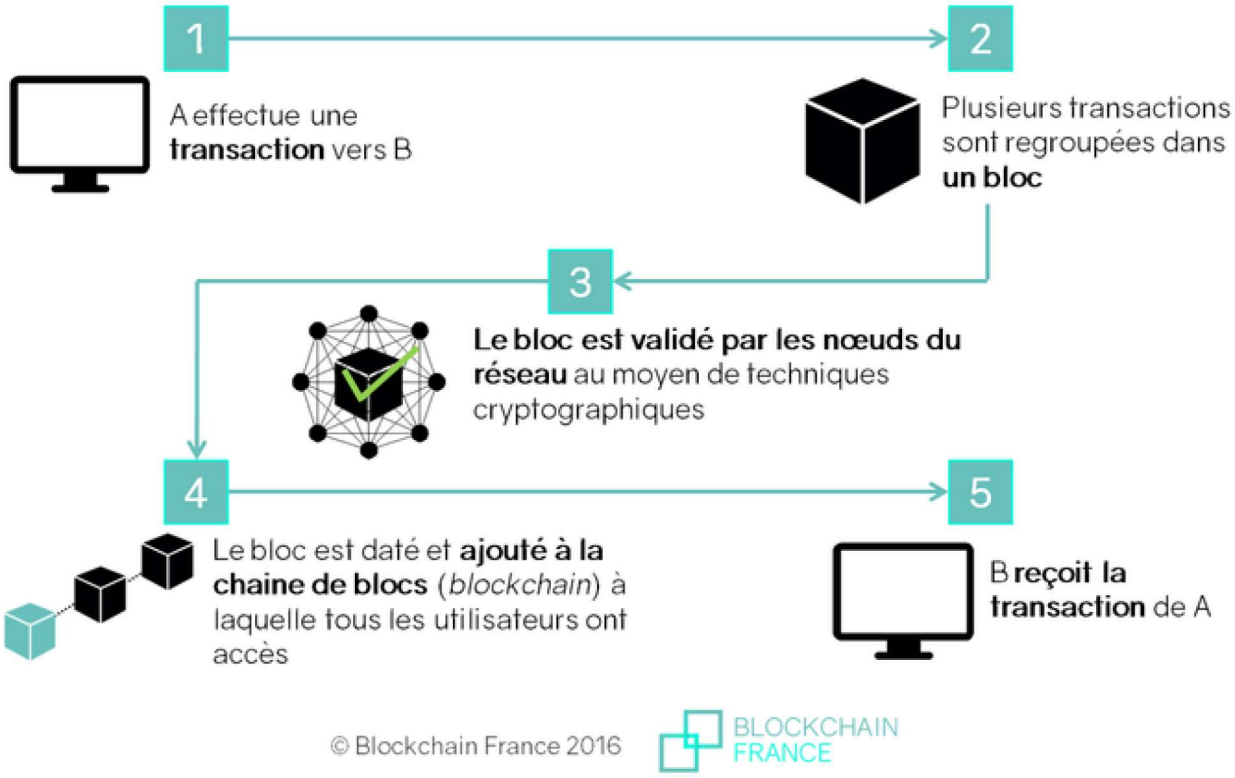
2.1.3.5.3.3 Comment ça marche ?

Voir vidéo aux liens : Blockchain emojis,

Comprendre la Blockchain visuellement (et simplement)

Toute blockchain publique fonctionne nécessairement avec une monnaie ou un token (jeton) programmable. Bitcoin est un exemple de monnaie programmable.
Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs. Chaque bloc est validé par les noeuds du réseau appelés les "mineurs", selon des techniques qui dépendent du type de blockchain. Dans la blockchain du bitcoin cette technique est appelée le "Proof-of-Work", preuve de travail, et consiste en la résolution de problèmes algorithmiques.

Une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau.



Ce processus prend un certain temps selon la blockchain dont on parle (environ une dizaine de minutes pour bitcoin, 15 secondes pour Ethereum).

2.1.3.5.3.4 Le potentiel de la blockchain

Ref : https://youtu.be/JID9c-MABis

Le caractère décentralisé de la blockchain, couplé avec sa sécurité et sa transparence, promet des applications bien plus larges que le domaine monétaire.Par exemple :

les applications pour le transfert d'actifs (utilisation monétaire, mais pas uniquement : titres, votes, actions, obligations…). Les applications de la blockchain en tant que registre : elle assure ainsi une meilleure traçabilité des produits et des actifs.

2.2 Les services de base du monde connecté

Pour nous permettre d'utiliser au mieux ce monde connecté ,il est essentiel de prendre connaissance des principaux sites web et les types de service de base qu'ils nous offrent.

Pour découvrir ces services de base, nous explorerons le recensement fait par wikipedia ici.

2.3 Les services étendus du monde connecté

L'arrivée des objets connectés et en particulier des assistants vocaux tels que : Alexa (produit par Amazon), Google Assistant, Djingo (opérateur orange), Ok-SFR (opérateur SFR), a fait apparaître des nouveaux services dans le monde connecté.

Nous appellerons « service étendus », ces services liés à l'apparition des objets connectés.

Ceux-ci vont nous permettre, dans les chapitres suivants, de créer nos propres services personnalisés en définissant des relations avec d'autres sites et avec nos propres objets connectés.

L'ensemble des objets connectés est souvent désigné sous le terme : IOT (Internet des objets).

Voir Introduction à l' Internet des objets.

2.3.1 De plus en plus d'objets connectés et de nouveaux services

Source : definition objet connecté

2.3.1.1 C'est quoi un objet connecté ?

Un objet connecté est tout simplement un objet : (montre,bracelet,balance etc..) ayant la faculté de communiquer via diverses mode de communication avec le monde qui l'entoure. La quasi totalité des objets peuvent devenir connectés ou communicants par exemple,une montre,un bracelet , une balance ,une maison. Un smartphone ou un PC par exemple est un objet connecté. Pour rendre un objet connecté ou communiquant,un des facteurs majeurs reste le réseau de communication,la plupart du temps sans fil (Wifi,Bluetooth,Li fi etc..).

2.3.1.2 Un objet connecté est en général composé d'objets connectés

Un **système de surveillance** composé d'objets connectés : détecteur de présence, camera...etc est lui même un objet connecté.

Une **maison connectée** qui contient des objets connectés : camera de surveillance, centrale d'alarme, volets roulants connectés par exemple est un objet connecté. Le terme de **smart Home** (***smart home***) est aussi utilisé pour désigner la maison connectée.

La **ville connectée** qui inclut des infrastructures publiques (bâtiments, mobiliers urbains, domotique, etc.), réseaux (eau, électricité, gaz, télécoms) ; transports (transports publics, routes

et voitures intelligentes, covoiturage, mobilités dites douces - à vélo, à pied, etc.) ; les e-services et e-administrations, est un objet connecté désigné aussi sous le terme de **smart city** (smart city).

La **planète terre** qui est surveillée en permanence par des satellites (mesure des gaz à effet de serre, de la température globale, du niveau de la mer) , des stations météos, des stations de détection sismiques etc..est un objet connecté.

2.3.1.3 Les objets connectés sont partout

Les objets connectés ont de plus en plus le vent en poupe et on les retrouve presque partout autour de nous.

2.3.1.3.1 Dans la maison

La figure ci-dessous comparée à la figure précédente illustre cette entrée croissante des objets connectés dans les foyers.

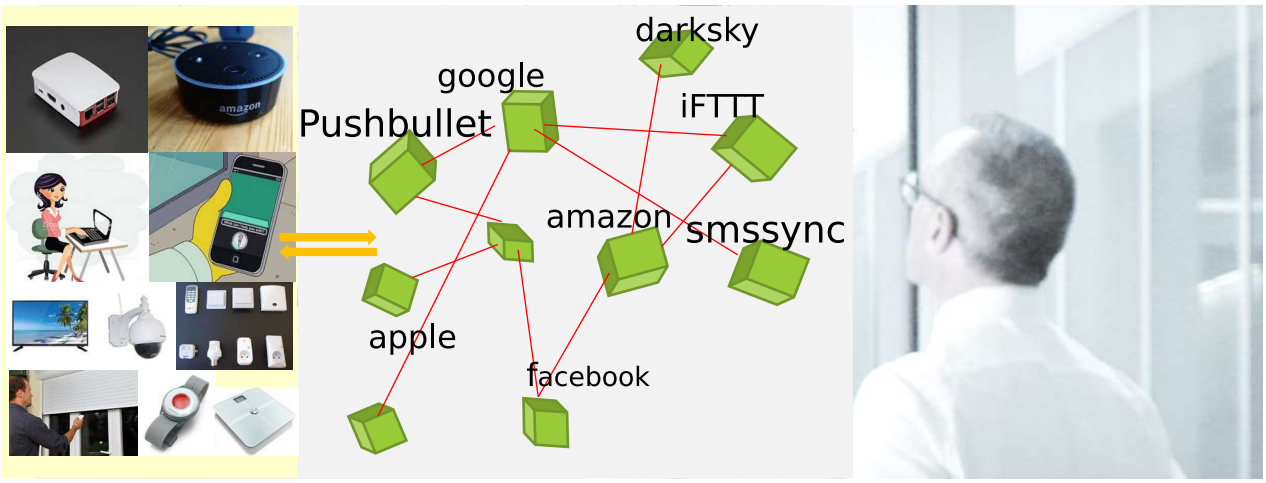


Illustration 18: Illustration du monde connecté dans le contexte des services étendus

Par exemple, nous y trouvons les objets connectés suivants :

- un micro ordinateur
- une enceinte vocale Alexa

- un ordinateur portable
- un smart phone
- une télévision connectée
- une camera de surveillance
- des équipements domotiques divers
- des volets roulants connectés
- une montre connectée
- une balance connectée

Nous trouvons également dans cette figure, des noms de sites web apparus avec les objets connectés ; par exemple : IFTTT, pushbullet, smssync...etc.

2.3.1.3.2 Dans la ville

La **smart city** (smart city).correspond au concept de ville connectée.

La smart city est un nouveau concept de développement urbain. Il s'agit d'améliorer la qualité de vie des citadins en rendant la ville plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets connectés et de services. Voir des exemples au chapitre précédent.

2.3.1.3.3 Sur soi

Le corps est devenu un objet connecté. Ref : CNIL_CAHIERS_IP2_WEB.pdf

2.3.2 Modèle pour se repérer dans le monde connecté étendu

Le schéma ci-dessous présente un modèle général du monde connecté étendu. Nous l'utiliserons dans les travaux pratiques proposés dans les chapitres suivants pour bien comprendre leurs fonctionnement.

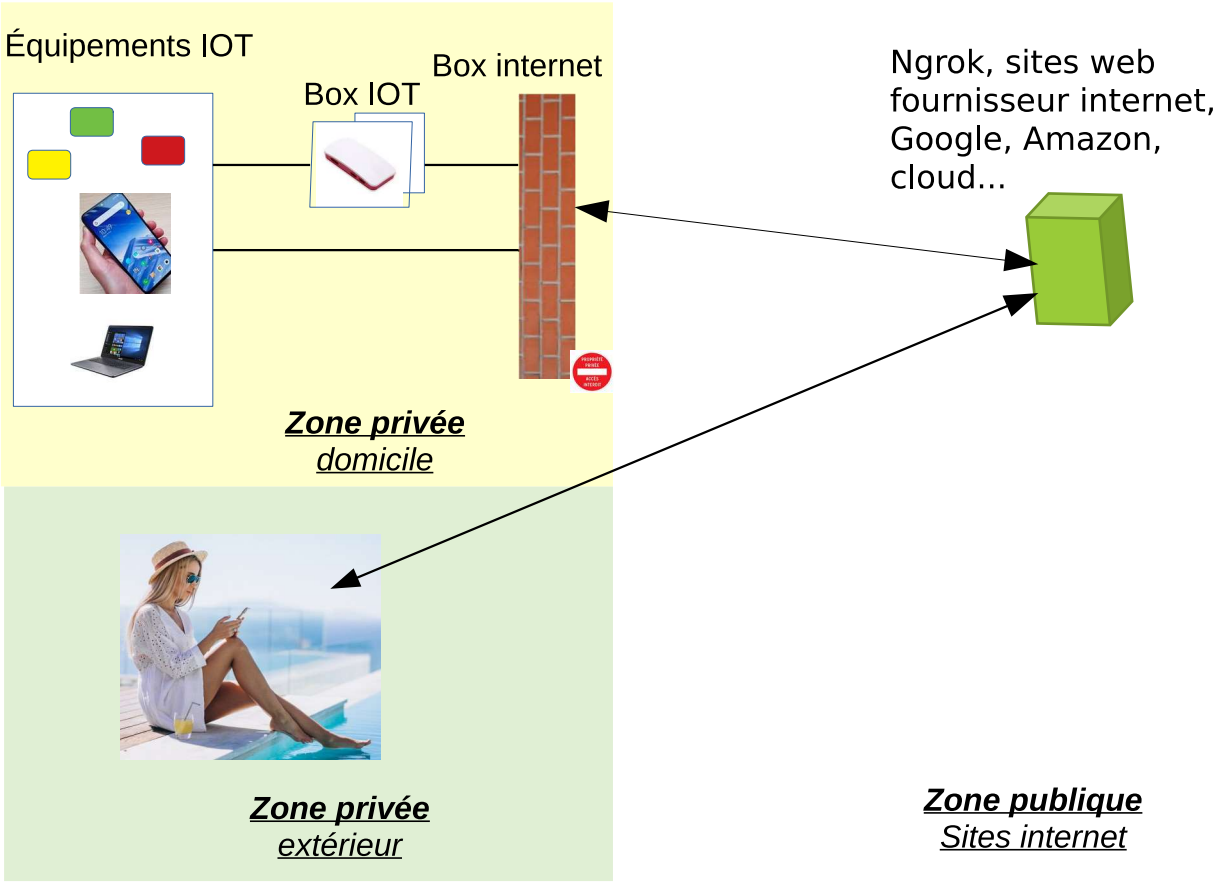


Illustration 19: Modèle général du monde connecté étendu

2.3.3 Découvertes des services étendus

2.3.3.1 Les assistants personnels et enceintes connectées

2.3.3.1.1 Alexa

Source : Wikipedia

Alexa est un logiciel de type assistant personnel intelligent développé par Amazon, rendu populaire par l'enceinte connecté Echo. Il est capable d'interaction vocale, de lire de la musique, faire des listes de tâches, régler des alarmes, lire des podcasts et des livres audio, et donner la météo, le trafic et d'autres informations en temps réel. Alexa peut également contrôler plusieurs appareils intelligents en faisant office de hub domotique.

Alexa a l'avantage d'être accessible sur de nombreuses machines qui ne sont pas des objets produits par Amazon. Il est aussi possible de lui ajouter des fonctionnalités, puisque la technologie est dite ouverte.

Illustration 20: Enceinte connectée echo dot (3e génération)

La figure suivante présente le principe de fonctionnement du service Alexa

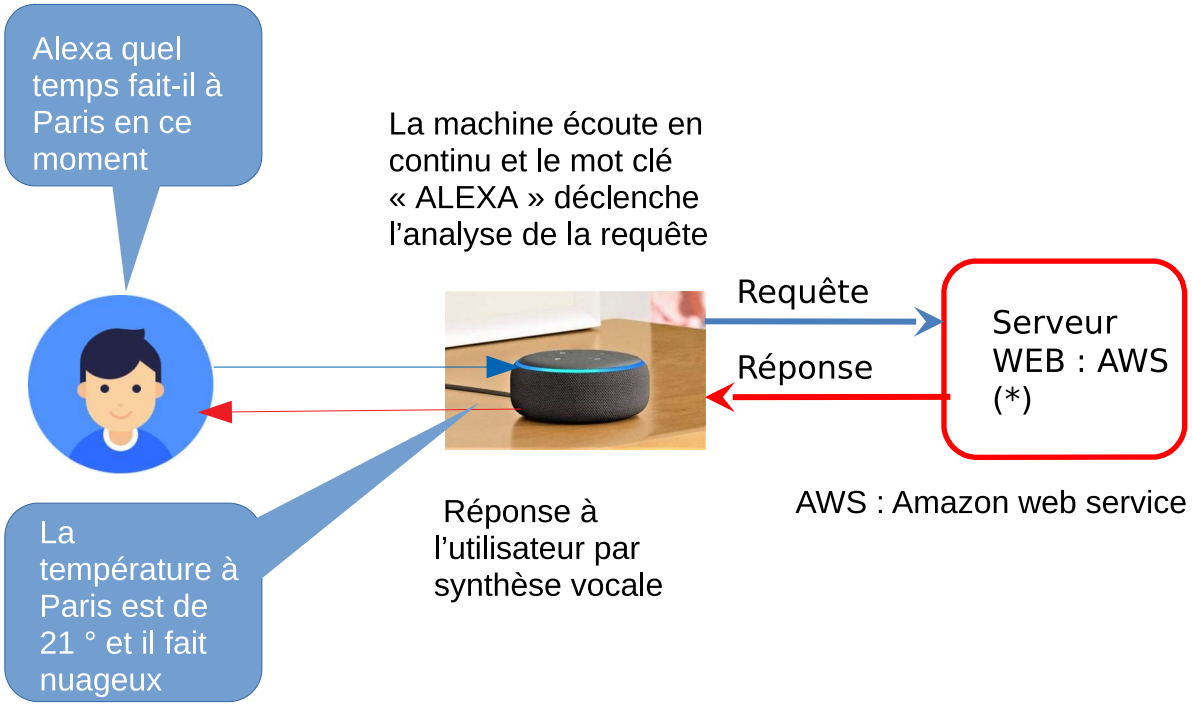


Illustration 21: principe de fonctionnement du service Alexa

Les skills c'est quoi ?

Source : Les skills, c'est quoi ?

Les skills d'Alexa sont similaires à la boutique d'application que vous pouvez retrouver sur votre smartphone Android ou iOS. Développées par des fabricants d'objets connectés ou des éditeurs tiers, les skills permettent d'enrichir votre expérience au quotidien en vous proposant de multiples fonctionnalités contrôlables par la voix, via Alexa.

Source : meilleurs skills

Les services offerts par ces skills se rangent en trois principales catégorie :

- skills-maison-connectee
- skills Musique, Radio et Audio
- skills Actualités

2.3.3.1.2 Google assistant

Google assistant est un logiciel de type assistant personnel intelligent développé par Google. Il a été lancé pour concurrencer le produit Alexa d'Amazon.

Google assistant peut être utilisé sur plusieurs produits de Google, qu'il s'agisse de smartphones Android compatibles, de téléviseurs Android TV, de l'assistant domestique Google Home, de montres Android Wear, etc. Notons également que Google Assistant est aussi disponible sous forme d'application pour les smartphone Apple. Voir complément d'information ici.

Illustration 22: Enceinte google home

À l'instar des skills d'Alexa, l'Assistant Google possède une bibliothèque de compétences que vous pouvez retrouver à l'adresse suivante depuis votre navigateur web

Des objectifs de développements ambitieux pour Google assistant

La prochaine étape est la conversation avec la machine. Cela signifie que vous n'avez pas besoin de dire « OK Google » pour démarrer une conversation avec Google assistant. L'assistant Google apprendra aussi à vous reconnaître par rapport à d'autres personnes présentes dans la pièce.

Les actions multiples sont également une nouvelle fonctionnalité qui vous permettent de demander plusieurs choses en même temps. La maîtrise des requêtes comme celle-ci est probablement ce qui va permettre à l'Assistant Google de devancer ses rivaux. De plus, un nouveau mode Pretty Please pour Google Assistant vous aidera à vous assurer que tout le monde dans votre foyer dit «s'il vous plaît» et «merci». Lorsqu'il est activé, il répond positivement lorsque vous dites l'une de ces phrases. Pretty Please peut être activé pour des membres spécifiques de votre famille. Ainsi, vous pouvez encourager vos enfants à être polis.

À l'avenir, Google affirme même que son Assistant sera en mesure d'appeler et de prendre rendez-vous pour vous. Découvrez Google Duplex ici.

La figure suivante présente le principe de fonctionnement de l'assistant Google installé sur une enceinte connectée google home

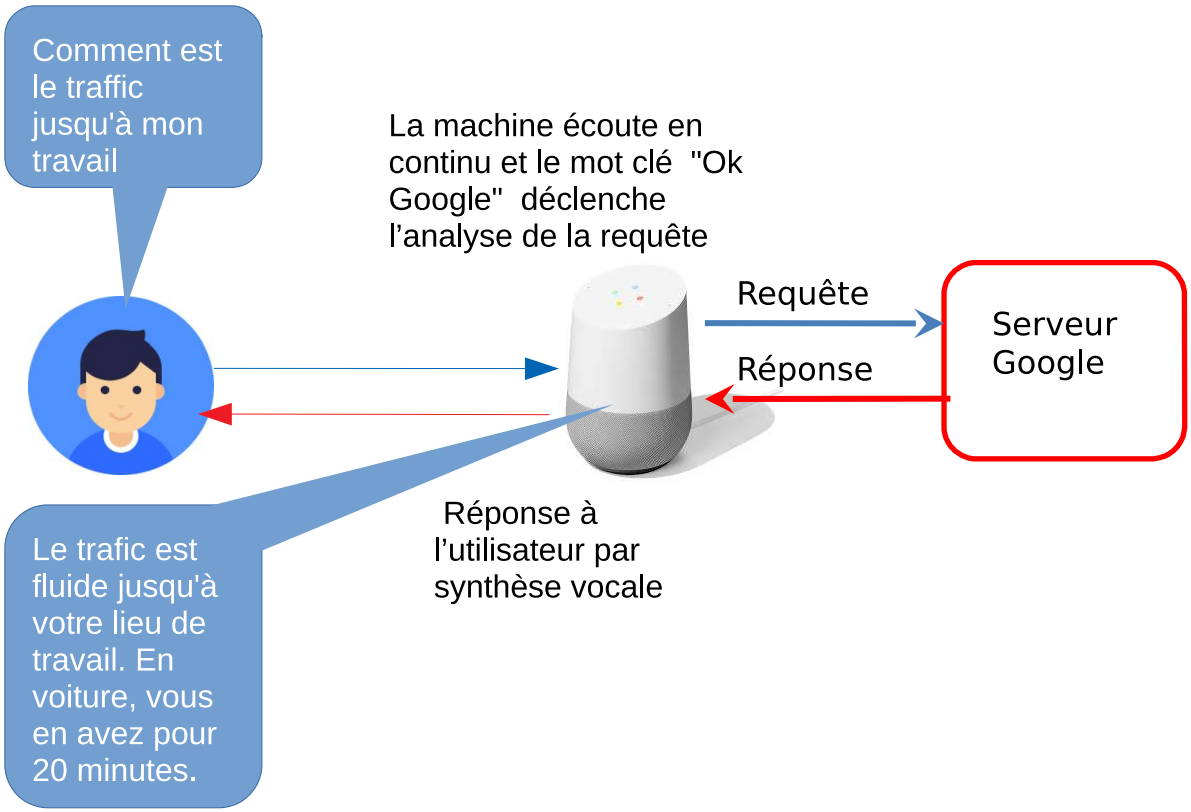


Illustration 23: principe de fonctionnement de l'assistant Google installé sur une enceinte connectée google home

2.3.3.1.3 Le contrôle des objets par les enceintes connectées

L'un des objectifs des enceintes connectés est de savoir contrôler par la voix tous les objets connectés de la maison présents et futurs vendus dans le commerce.

En 2019 par exemple , Google , estimait que son Assistant était compatible avec « *plus de 10 000 appareils connectés fabriqués par plus de 1 000 marques* ».

L'article ici présente un catalogue non exhaustif de ces appareils connectés commandables par la voix .

Pour suivre constamment cette évolution, les enceintes connectées sont mises à jour périodiquement. Ces mises à jour sont automatiques et sans intervention manuelle.

Exemple d'installation "Connecter sa porte de garage à Google Assistant pour une quinzaine d'euros" sur YouTube

2.3.3.2 ImperiHome : Gestion des objets connectés et de la ville connectée

Source : http://www.mtom-mag.com/article5356.html

Imperihome est une application (= client web) disponible sur Google Play et Apple store. Elle permet aux utilisateurs d'accéder aux données de leur ville connectée (smart city), de leur environnement proche et aussi contrôler tous les objets connectés au sein de leurs foyers.

Dans l'univers de la **Smart City**, l'application intègre les données de la qualité de l'air (Prev'Air - France, AirNow-USA & Canada, European Environment Agency – Europe), de la mobilité urbaine (Velib-Paris, Citibike-New York, Velo'v-Lyon, Vélo Bleu-Nice, Autolib-Paris, Parking-Lyon….). De nouveaux services seront intégrés prochainement et les utilisateurs accéderont aux données de leur consommation d'énergie (eau, gaz, électricité…).

L'application permet de manager les plus grands marques d'objets connectés et de box domotiques grand public : Wink, Vera, Fibaro, Zipato, Jeedom, Eedomus, Homeseer, Nest, Nokia Health, Philips Hue, LIFX, Myfox, Netatmo, Fitbit, Xee, Yeelight, Sonos….

Nota : **Imperihome** peut s'interfacer avec le **serveur web domoticz**. Voir explication et schéma de fonctionnement ici.

Chaque utilisateur peut construire sa propre interface au sein de son Smart Phone ou de sa tablette qui gère à distance de multiples sites comme son domicile, sa résidence secondaire, le domicile de ses grands-parents dont il s'occupe, ou son bureau.

l'application est gratuite. On peut souscrire aussi à un service Premium payant sans engagement de durée.

ImperiHome est disponible en Français, Anglais sous Android et iOS et en Allemand, Espagnol et Italien pour la version Android uniquement.

2.3.3.3 Darsky : les informations météos de l'objet connecté planète terre

Le site https://maps.darksky.net fournit les données météo de l'objet connecté 'planète terre' .

Allons visiter ce site en suivant le parcours ci-dessous

1-se connecter au site et se positionner sur Bretigny sur orge

2-visualiser sur la carte les différents données météo : temperature, précipition, vents..

3-obtenir des données météo en utilisant l'API. ref : https://darksky.net/dev/docs

Depuis un navigateur, faire la requête :

https://api.darksky.net/forecast/[key]/[latitude],[longitude]

*Nota : La **latitude** de la ville de Brétigny-sur-Orge est 48.6167 et la **longitude** de la ville de Brétigny-sur-Orge est 2.3167*

La requête est : https://api.darksky.net/forecast/[key]/48.6167,2.3167

Nota 1: Le paramètre 'key' est obtenu en s'inscrivant sur le site Darksky.

Nota 2 : Le temps indiqué est indiqué en nombre de secondes écoulées depuis le 1er janvier 1970 à minuit UTC précise. Voir : http://timestamp.fr/?

2.3.3.4 IFTTT : un site web pour vous rendre beaucoup de petits services

IFTTT est le sigle de **IF T**his **T**hen **T**hat c'est à dire : **Si Ceci Alors Cela ()**

IFTTT est un service Web gratuit à qui on peut demander de nous rendre des petits services. Quelques exemples de services :

S'il pleut demain, rappelle moi de prendre un parapluie. S'il va pleuvoir demain, IFTTT va vous envoyer un notification sur votre smart phone,

Envoie un SMS à mes parents dès que je suis rentré de l'école. Lorsque le smartphone de votre enfant se reconnecte au wifi de la maison, IFTTT détecte que l'enfant est rentré à la maison et il vous envoi un SMS,

Attente de sortie de ma valise du tapis roulant de l'aéroport. Envoie moi un sms dès que ma valise se reconnecte au réseau wifi créer avec mon smarthone,

Dès que je prend une photo avec mon smart phone, envoie la sur google drive.

Dès qu'un nouveau fichier est créé dans un répertoire de google drive envoi une notification vers les smartphones de plusieurs personnes

M’envoyer un mail contenant ma localisation pour que je sache retrouver mon chemin au retour.

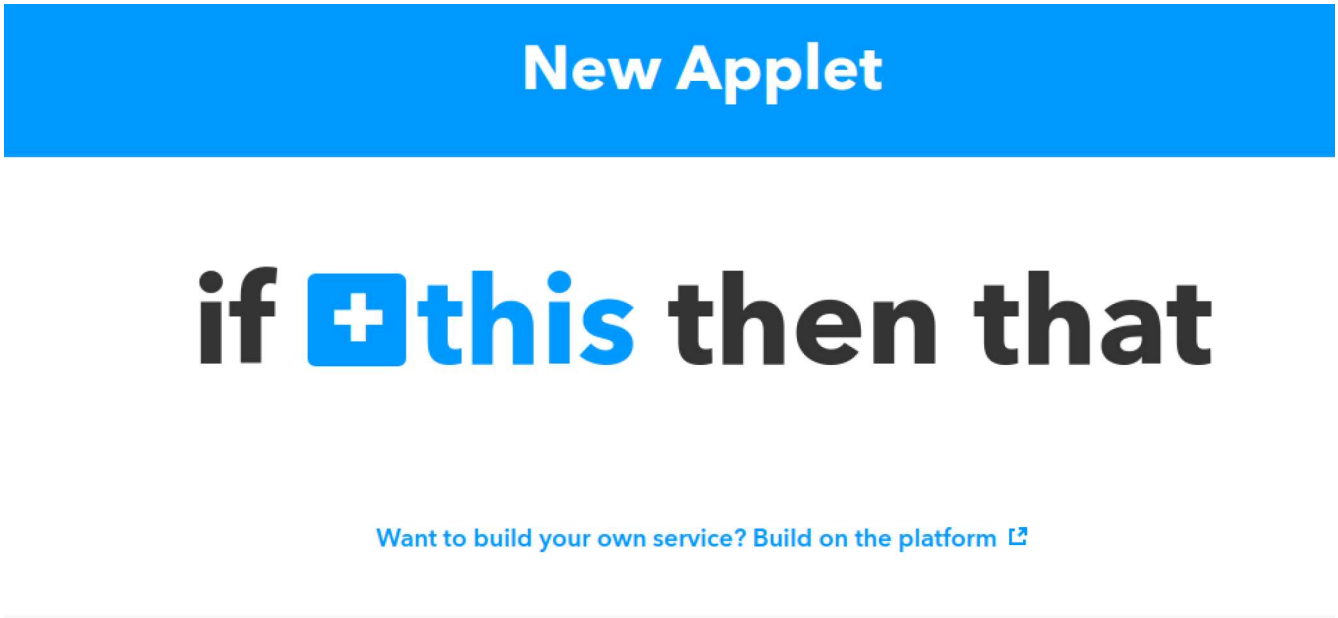
2.3.3.4.1 Exemple de création d’un service dans IFTTT

Pour expliquer comment ajouter un service dans IFTTT, nous allons créer l’exemple **:**

2.3.3.4.1.1 « Envoie automatique d’un SMS à mes parents dès que je suis rentré de l’école »

Se référer aux figures ci-dessous pour avoir une vue globale du système à créer.

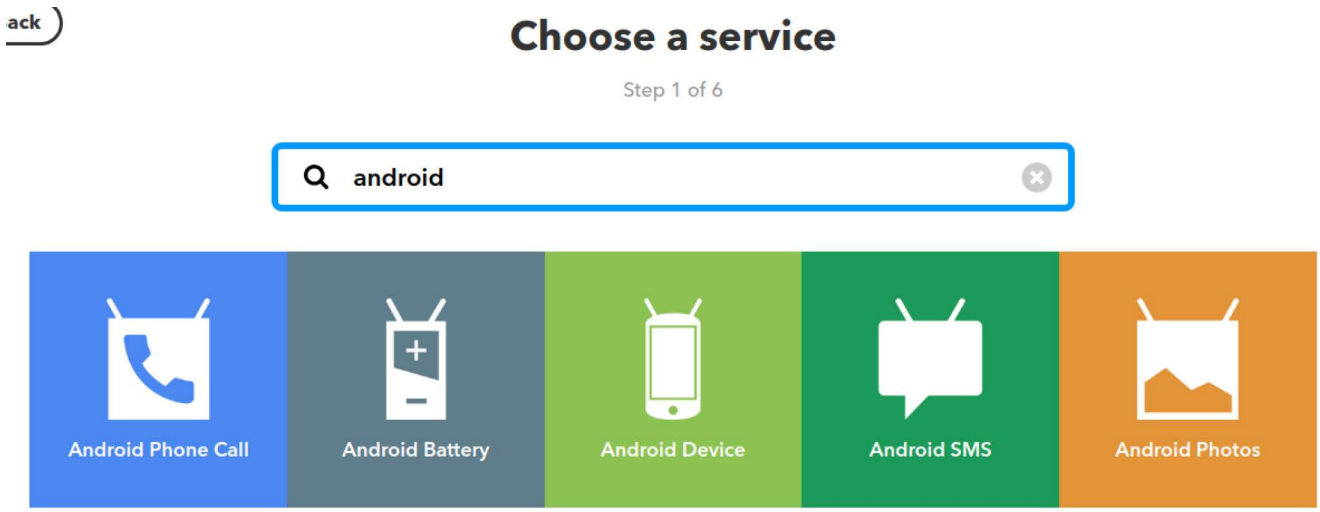
Commencez par vous rendre sur la plateforme (site web IFTTT) puis, créez un compte ici. Une fois fait, vous allez pouvoir, dans votre compte, cliquer sur “New Applet”. Et donc arriver sur cet écran :



Cliquer sur le +

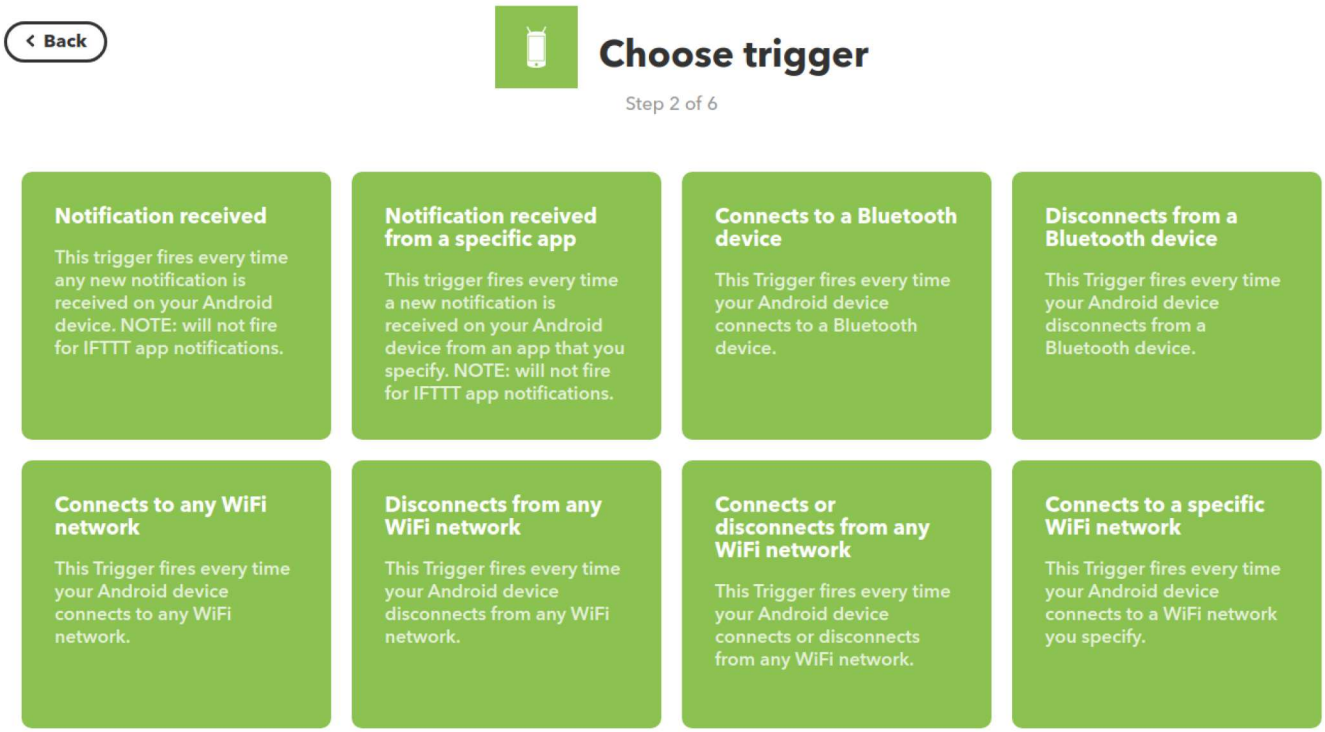
2.3.3.4.1.2 Suivez les 6 étapes illustrées ci-dessous.

étape N° 1

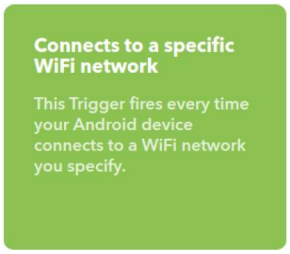


Cliquer sur Android Device 

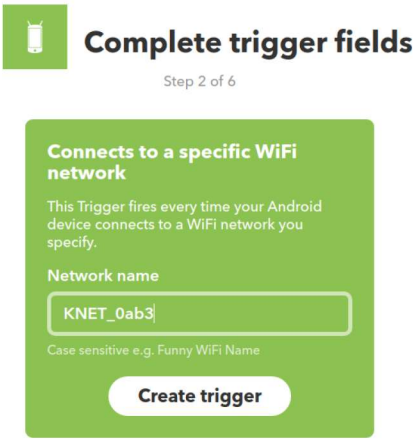
étape N°2



Cliquer sur



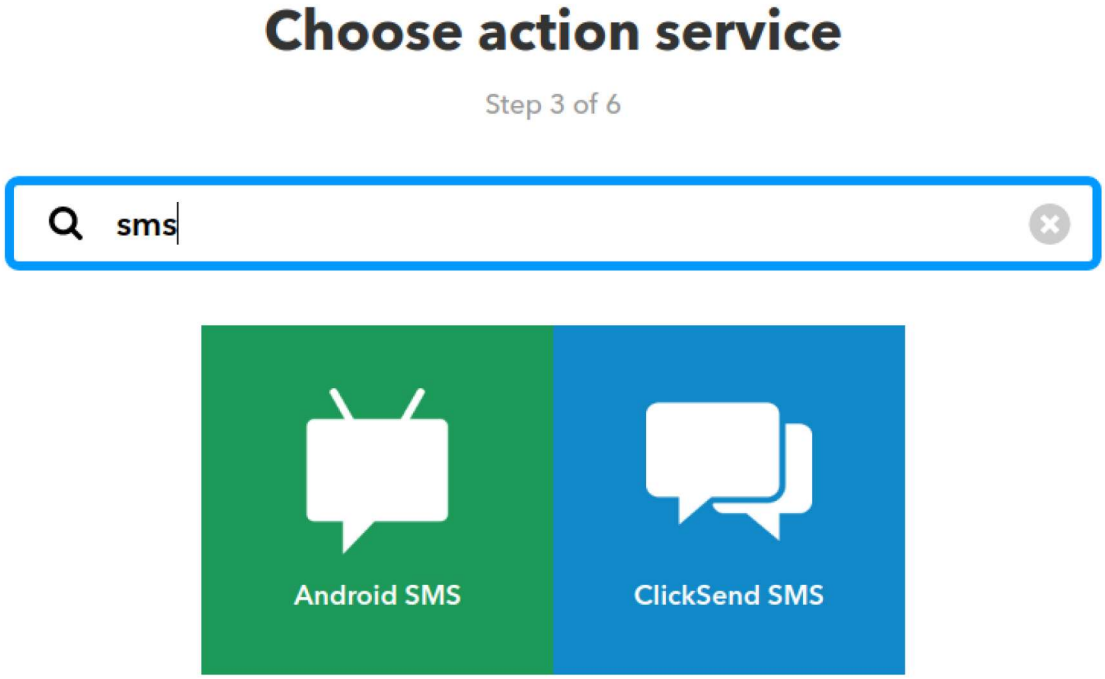
Entrer le nom du réseau wifi , exemple : KNET_0ab3



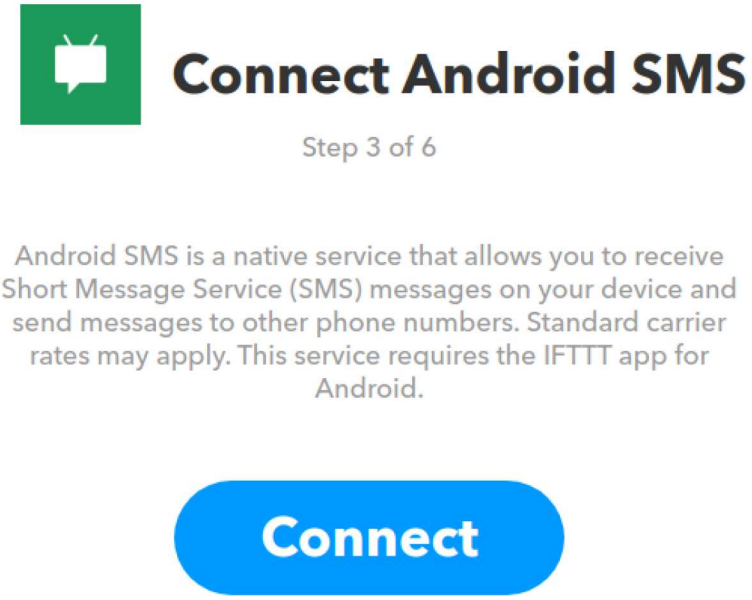
puis cliquer sur « Create trigger

Cliquer sur le +

étape N°3

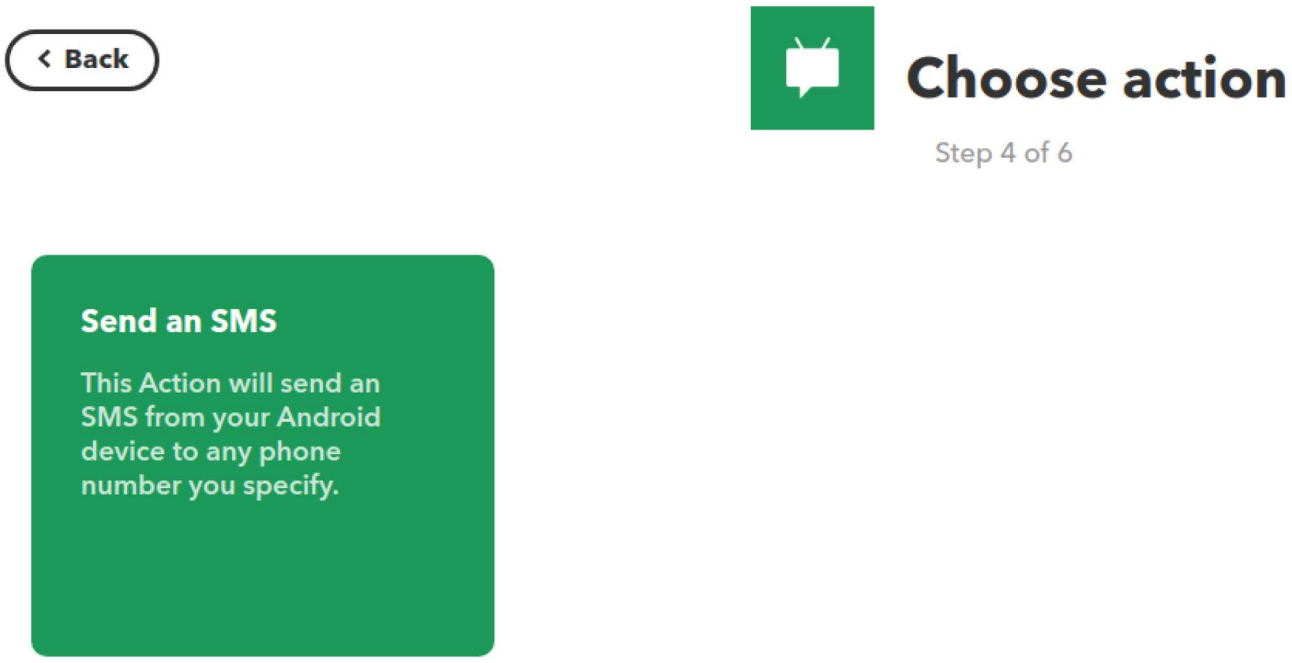


cliquer sur «Android SMS»



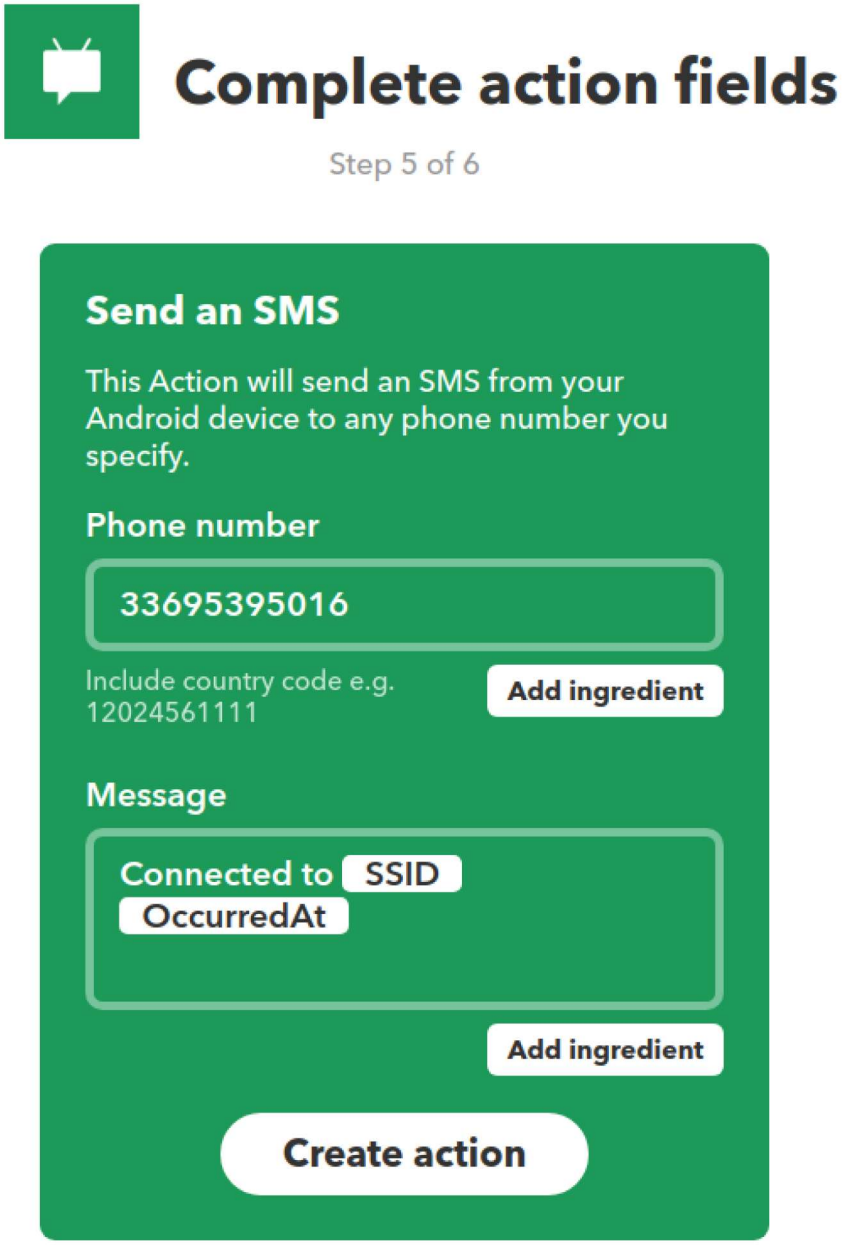
Cliquer sur Connect

étape N°4



étape N°5

Cliquer sur « Send an SMS ».



Cliquer sur « create action ».

étape N°6

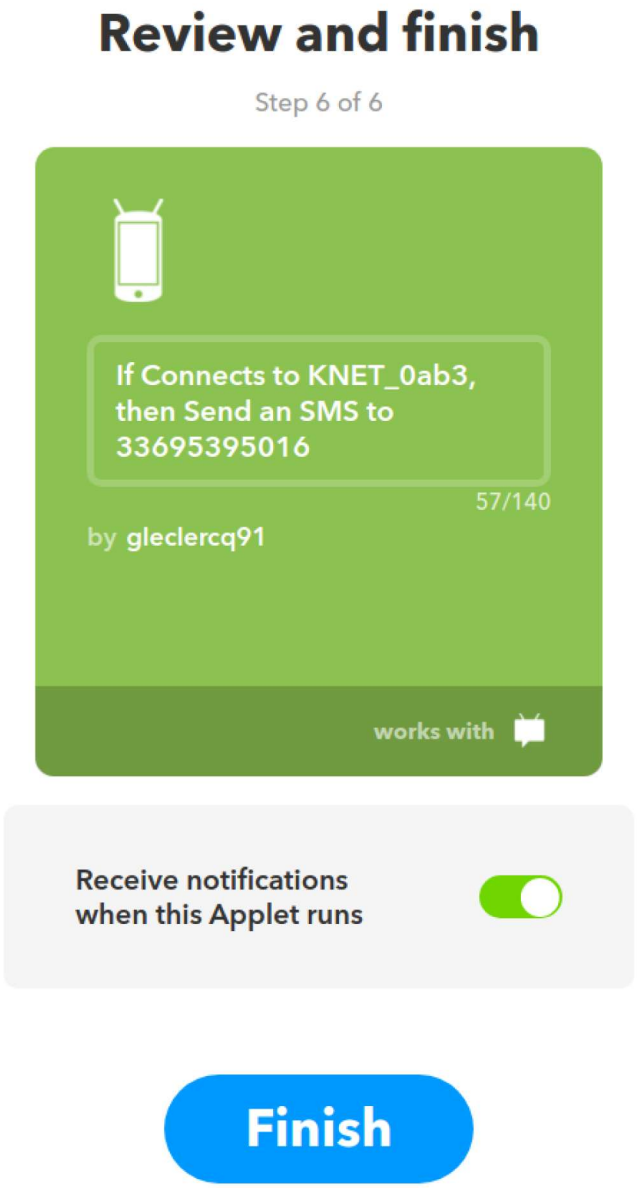


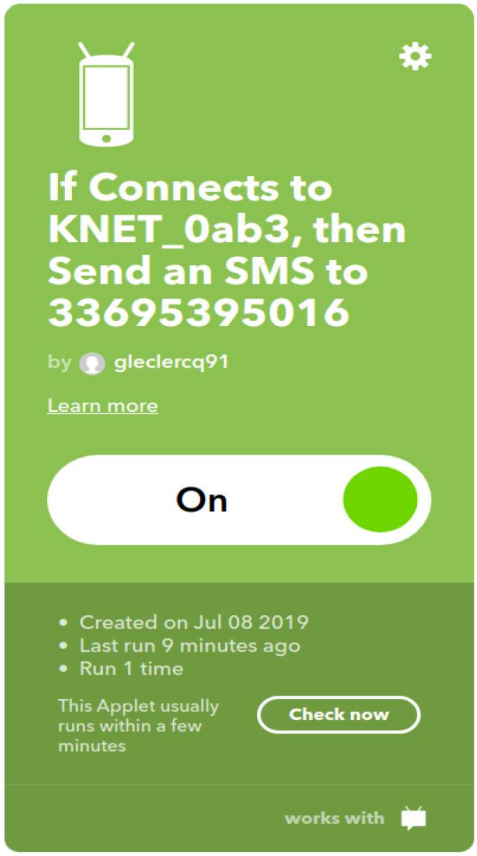
Illustration 24: principe de fonctionnement de l'assistant Google installé sur une enceinte connectée google home

2.3.3.4.1.3 Comment tester le bon fonctionnement du service ?

- déconnectez le smart phone du wifi puis reconnectez le sur le réseau wifi.
- Vous recevrez le sms : « Connected to Knet_0ab3 July 08, 2019 at 04:58PM ».

Le résultat est conforme au service demandé.

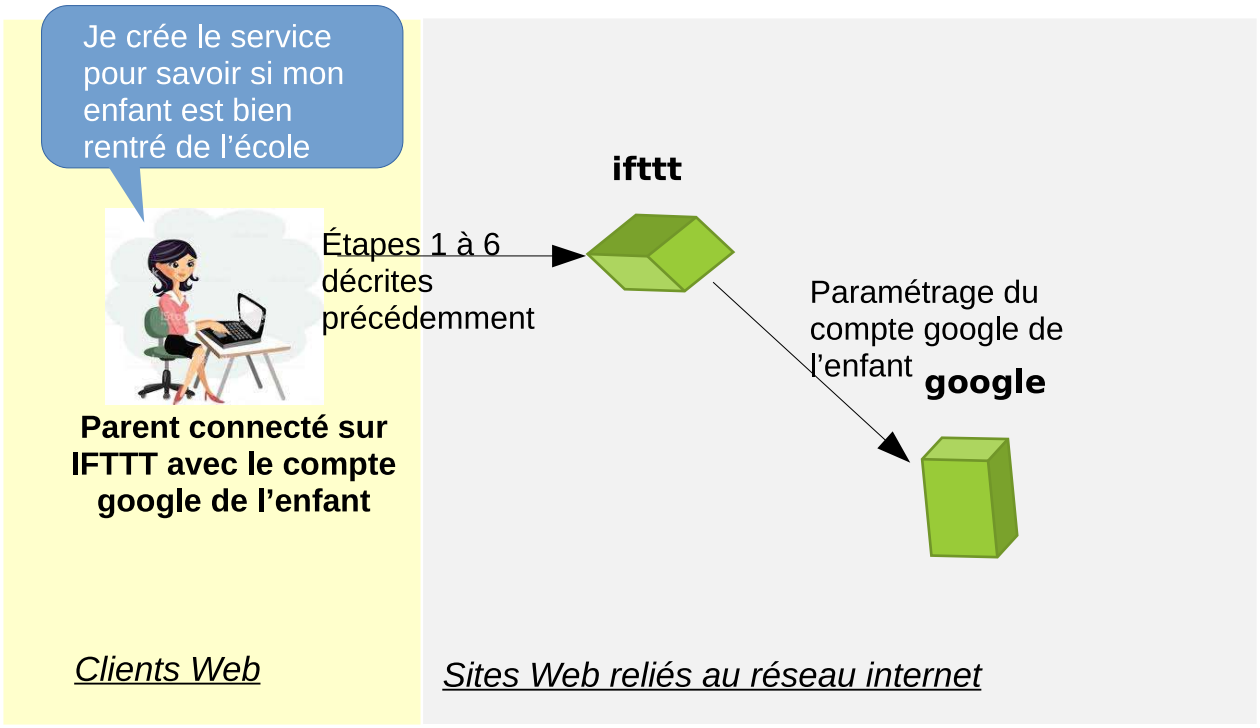
Le service fonctionnera tant qu'il n'a pas été désactivé.



2.3.3.4.1.4 Pour désactiver le service, cliquer sur « ON »

2.3.3.4.1.5 Pour modifier le service, cliquer sur …. 

2.3.3.4.1.6 Modèle de flux lors de la création du service



2. *Illustration 25: IFTTT Modèle de flux lors de la création du service*

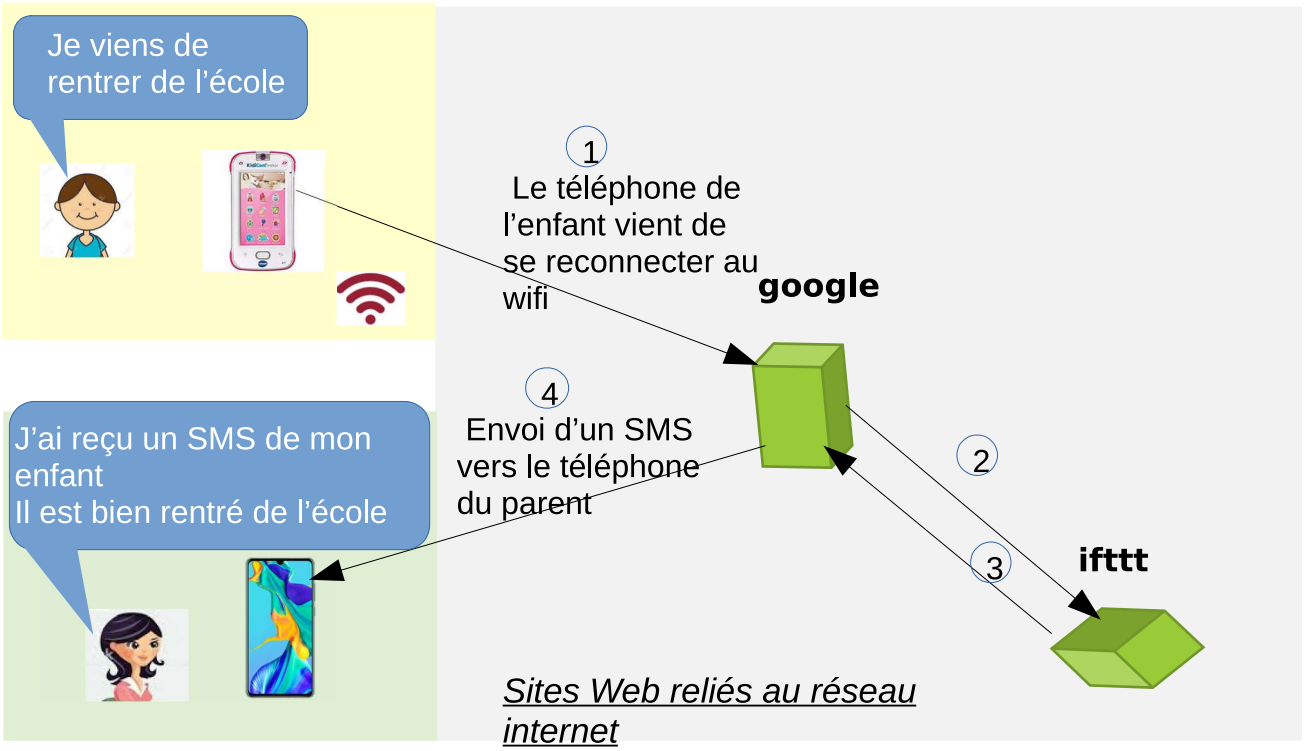


Illustration 26: IFTTT Modèle de flux lors de l'utilisation du service

2.3.3.4.2 Nota : Modèle de flux équivalent sans usage de IFTTT

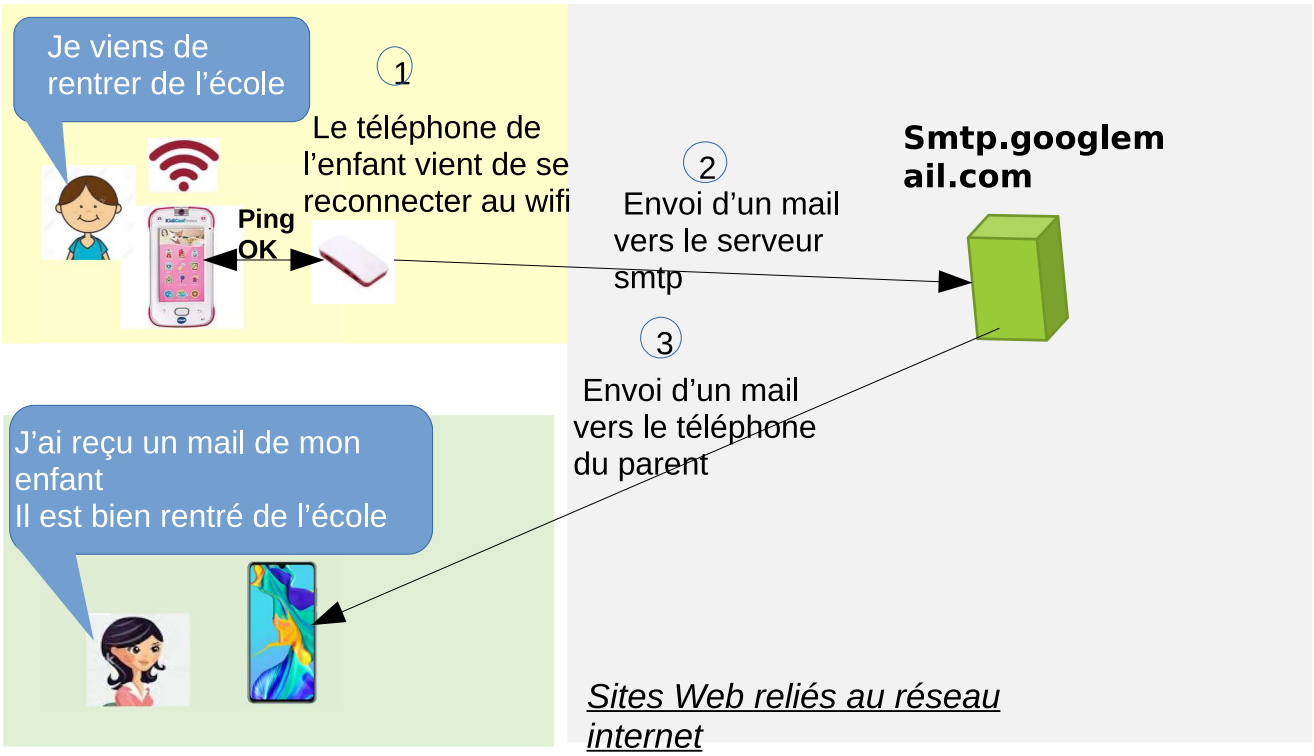


Illustration 27: Modèle de flux équivalent sans usage de IFTTT

2.3.3.4.3 Documents complémentaires sur IFTTT

Comment bien utiliser IFTTT pour son domicile

IFTTT _ comment ça marche _ Nos meilleures applets_recettes

Comment automatiser des apps et services

2.3.3.5 Ngrok : l'outil qui vous permet d'accéder à vos objets connectés depuis le bout du monde

2.3.3.5.1 Puis-je contrôler mes volets roulants par l'internet depuis le bout du monde ?

Les commandes destinées à un appareil connecté, par exemple : un aspirateur, un volet roulant passent :

- par l'interface utilisateur d'une application mobile ou un navigateur, c'est à dire d'un client web ,
- puis le sur le réseau local, qui constitue en fait un internet local, jusqu' au serveur web de l'appareil qui est en général dans l'appareil lui-même.
- Le serveur web va ensuite « relayer » la commande à l'appareil, c'est à dire par exemple aux moteurs, interrupteurs, lampes de l'appareil.

La question qu'un utilisateur peut se poser est : Puis-je contrôler mon appareil à distance par l'internet depuis le bout du monde ?

2.3.3.5.2 La réponse classique est « oui, mais il faut configurer la box internet et ceci n'est pas recommandé».

En effet, les appareils connectés au réseau local sont protégés par la box internet (appelé aussi « routeur ») contre les tentatives d'intrusion qui pourraient provenir de l'internet. Ceci signifie qu'il n'est pas possible normalement d'envoyer à distance, depuis l'internet, une commande à un objet connecté.

Il est néanmoins en général possible de configurer la box internet pour autoriser ces accès. Cela s'appelle : « mise en place d'un port forwarding ». Elle consiste à autoriser l'accès, depuis l'internet, d'un port particulier sur le réseau local. Cette technique n'est pas recommandée car elle rend le réseau local vulnérable aux tentatives d'intrusions qui sont très nombreuses sur l'internet.

2.3.3.5.3 Ngrok : une solution sécurisée qui permet de contrôler vos objets depuis le bout du monde

Ngrok est un logiciel couplé à un service web qui va vous permettre de créer un tunnel (VPN) à partir d'un accès internet vers un port sur votre machine en local.

Ngrok est installable sur linux, windows et mac.os.

L'intérêt principal de cette solution est qu'elle évite toute intervention sur la box internet du réseau local du lieu qui héberge vos objets connectés. De plus, elle vous permet d'accéder à vos objets connectés depuis le bout du monde selon une connexion chiffrée. Voir HTTPS.

2.3.3.5.4 Exemple d'emploi

La figure ci-dessous présente le fonctionnement de ngrok appliqué à un exemple simple de télécommande de volets roulants.

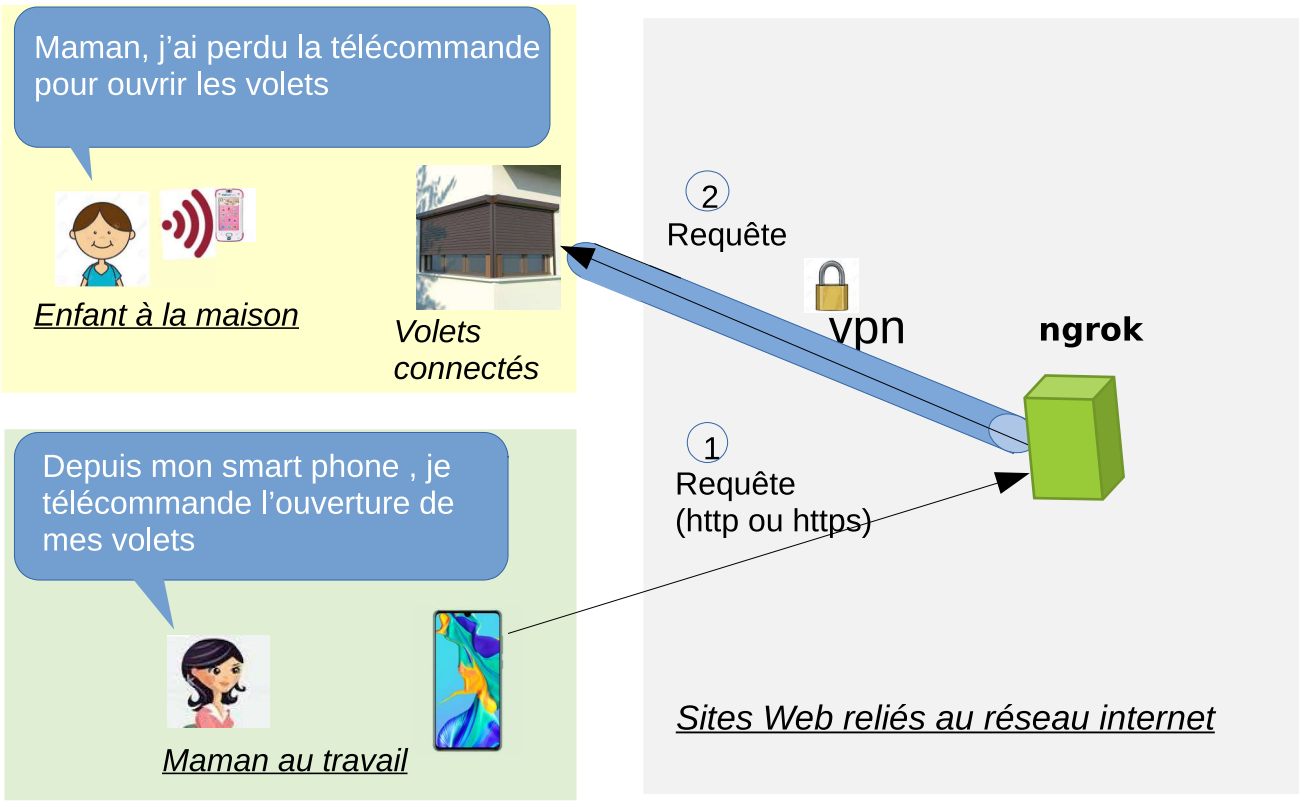


Illustration 28: NGROK ngrok appliqué à un exemple simple de télécommande de volets roulants

La mère de l'enfant, qui est absente du domicile, peut télécommander l'ouverture des volets roulants à partir de son smart phone par exemple.

Pour télécommander ses volets roulants,elle rentre la commande sur son navigateur depuis son smart phone ou PC :

- https://9b91ebdb.ngrok.io/ouvrir-volets pour ouvrir les volets

- https://9b91ebdb.ngrok.io/fermer-volets pour fermer les volets

La commande est envoyée vers le site web ngrok qui la renvoi à travers le vpn qui a été établi avec l'application client ngrok (=client web). Cette application est installée par exemple dans un objet connecté « micro ordinateur » (rasperry zero). L'application ngrok relaye ensuite cette commande vers le logiciel serveur web de l'objet connecté « micro ordinateur ». Celui-ci envoi alors un signal électrique aux volets roulant correspondant à la commande.

2.3.3.5.5 Démonstration pratique de ngrok

2.3.3.5.5.1 Objectif de cette démonstration

Nous verrons à travers cette démonstration qu'à partir d'un smartphone connecté sur l'internet public, il nous est possible de commander l'ouverture ou fermeture des volets, c'est à dire l'allumage ou l'extinction des leds

2.3.3.5.5.2 Configuration

On utilise un simulateur de télécommande de volets roulants composé de :

- un micro ordinateur Raspberry pi 3
- deux Leds pour simuler des bouton poussoir qui commandent respectivement : l'ouverture des volets et la fermeture des volets.

Les logiciels installés dans le Raspberry pi 3 sont : ngrok (client ngrok) et un serveur web : ''server_allumer_led.py ''.

Voir la maquette de simulation « serveur web maquette » ci-dessous.

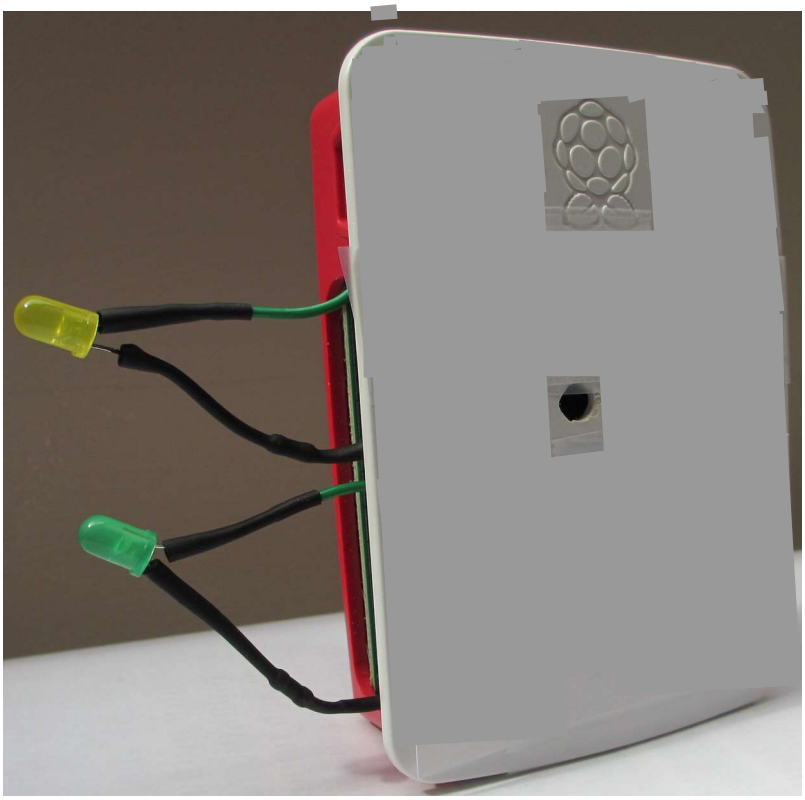


Illustration 29: serveur web maquette hébergé dans un raspberry pi

2.3.3.5.5.3 mise en œuvre

Lancement sur le raspberry pi du serveur Web : ‘’server_allumer_led.py ‘’

A partir d’un terminal ssh (sur linux) ou putty (sur windows), lancer le serveur web avec la commande :

python3 server_allumer_led.py

vérifier qu’à partir d’un navigateur tel que chrome ou Mozilla Firefox par exemple, que le serveur web fonctionne.

Par exemple, si on appelle l’url :

http://192.168.1.27:5000/Led-verte

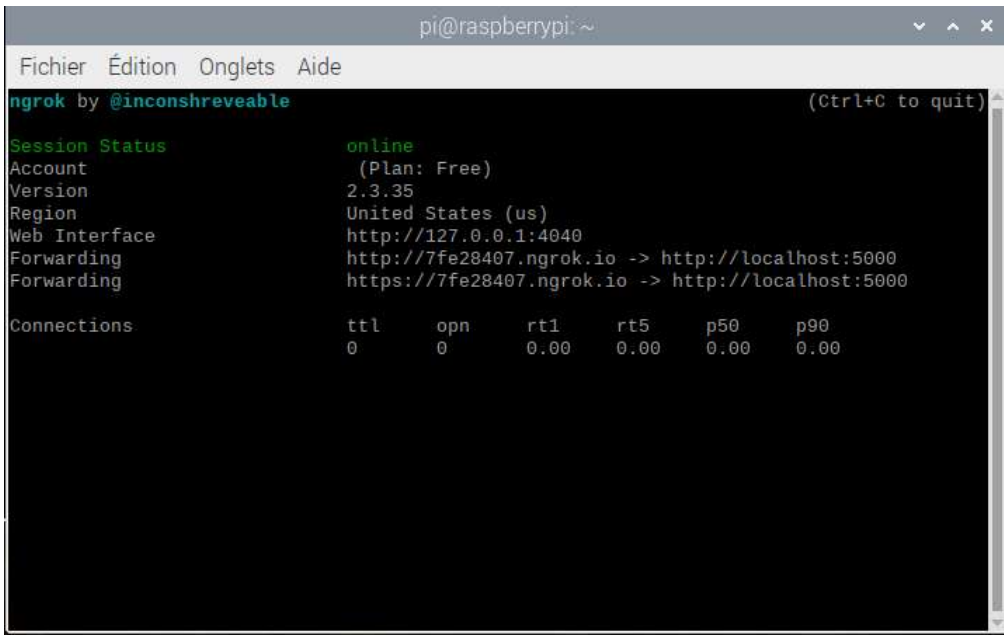
la led verte s’éteint ou s’allume à chaque envoi de cette commande.

Établissement du tunnel ngrok

Ouvrir un terminal sur le raspberry pi puis lancer la commande :

./ngrok http 5000

Le résultat qui apparaît dans le terminal est présenté ci-dessous



Vérification du bon fonctionnement de la commande à partir d'un smartphone connecté sur l'internet public.

Vérifier en entrant l'url :

https://7fe28407.ngrok.io/Led-verte

dans un navigateur tel que chrome ou Mozilla Firefox lancé depuis, par exemple, un smart phone connecté sur un réseau public, que le serveur web fonctionne.

La led verte s'éteint ou s'allume à chaque envoi de cette commande.

2.3.3.5.6 Alternative à ngrok

Le logiciel serveo est une alternative à nrok. L'un des avantages par rapport à ngrok est qu'il ne nécessite pas d'installer un logiciel dans le micro ordinateur (du type du « client ngrok ») car il utilise le serveur ssh du micro-ordinateur.

2.3.3.6 Webhook l'outil qui informe les autres site web si un évènement se produit

2.3.3.6.1 C'est quoi un Webhook ?

Le terme « Webhook » désigne un mécanisme intégré dans un site web dont la fonction est d'envoyer une requête vers un autre site web pour déclencher une action ou obtenir une information.

Ceci permet d'automatiser des actions entre différents sites web.

Citons quelques exemples de services qui utilisent le Webhook :

- IFTTT exemple d'emploi : s'il pleut alors envoyer la requête «enrouler le store » à mon objet connecté « store ».
- Dropbox exemple d'emploi : si un nouveau fichier intitulé : « enrouler le store » est créé dans mon dropbox, alors envoyer la requête «enrouler le store » à mon objet connecté « store »
- Zapier exemple d'emploi : si je reçois un nouveau mail dont l'expéditeur est : « dupont » alors ranger l'information dans l'une des applications de google drive.
- Facebook : https://developers.facebook.com/docs/pages/realtime/
- gmail : https://developers.google.com/gmail/api/guides/push
- twitter : https://developer.twitter.com/en/docs/accounts-and-users/subscribe-account-activity/guides/getting-started-with-webhooks

2.3.3.6.2 Démontration Webhook: demander à mon enceinte vocale de fermer ou ouvrir mes volets

Cette démonstration est une variante de la démonstration précédente. Elle utilise le même site web ''server_allumer_led.py '' hébergé sur le raspberry pi.

La différence est que le smart phone est remplacé par une enceinte connectée Alexa et on utilise le mécanisme Webhook du site IFTTT.

L'enceinte Alexa est connectée par wifi à l'internet.

Le modèle de flux est détaillé en figure ci dessous.

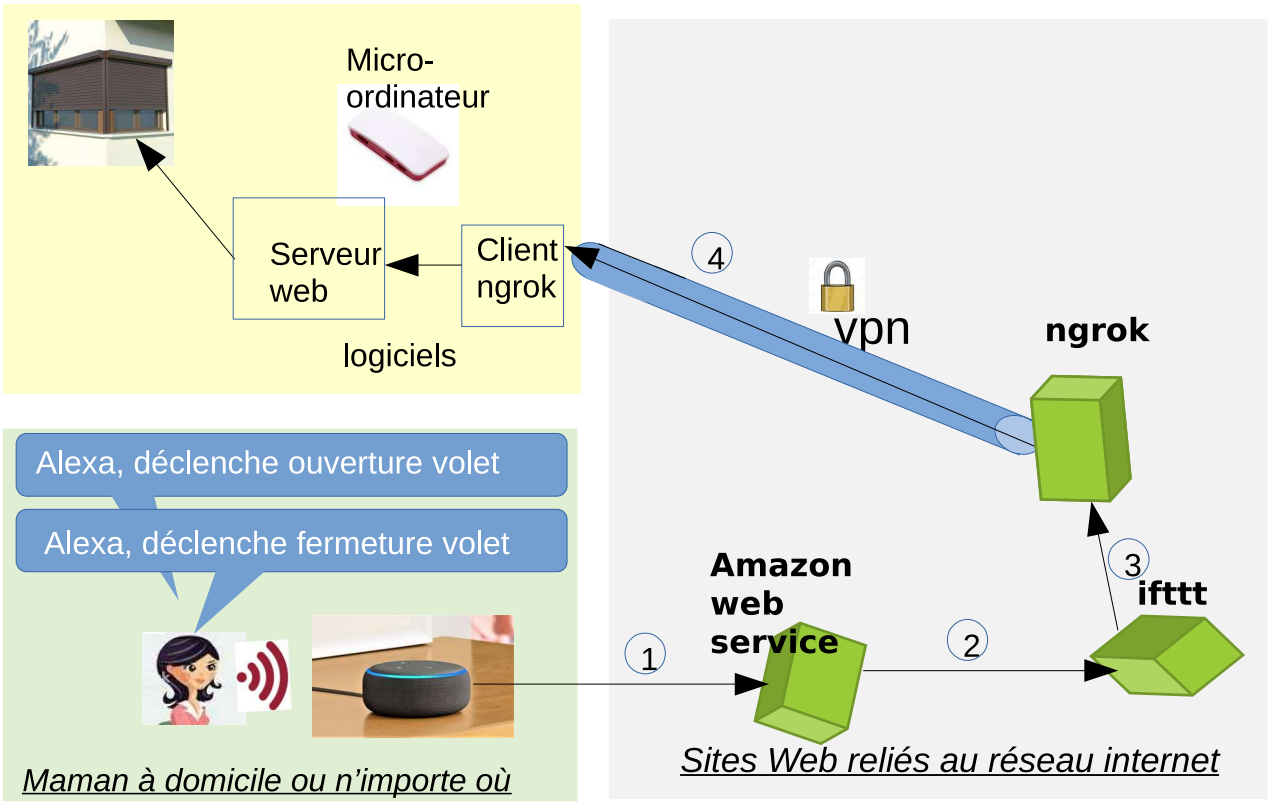


Illustration 30: Démontration Webhook avec enceinte Amazon Echo

Les services (= applets) IFTTT utilisés sont présentés ci-dessous.

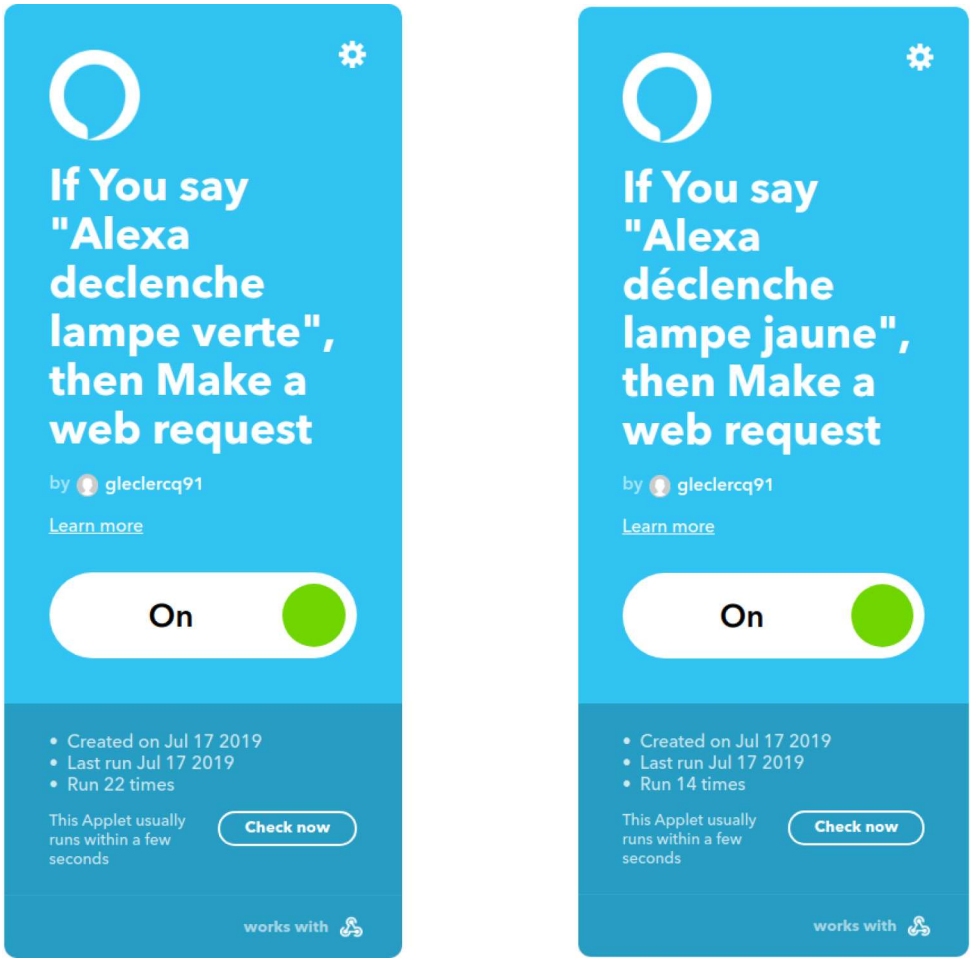


Illustration 31: services (= applets) IFTTT utilisés pour demonstration webhook

2.3.3.7 Le Broker MQTT : un type de site internet constituant un réseau au dessus d'internet

ref : wikipedia

MQTT1 (Message Queuing Telemetry Transport2) est un protocole de messagerie publish-subscribe basé sur le protocole TCP/IP.

Il a été initialement conçu en 1999 pour connecter pour connecter des oléoducs sur des réseaux satellites non fiables. L'objectif était d'avoir un protocole efficace en bande passante, léger et utilisant peu d'énergie de batterie, car les appareils étaient connectés par liaison satellite et à cette époque c'était extrêmement coûteux.

Un « Broker MQTT » constitue à lui seul un réseau de communication au dessus de l'internet, basé sur le protocole MQTT.

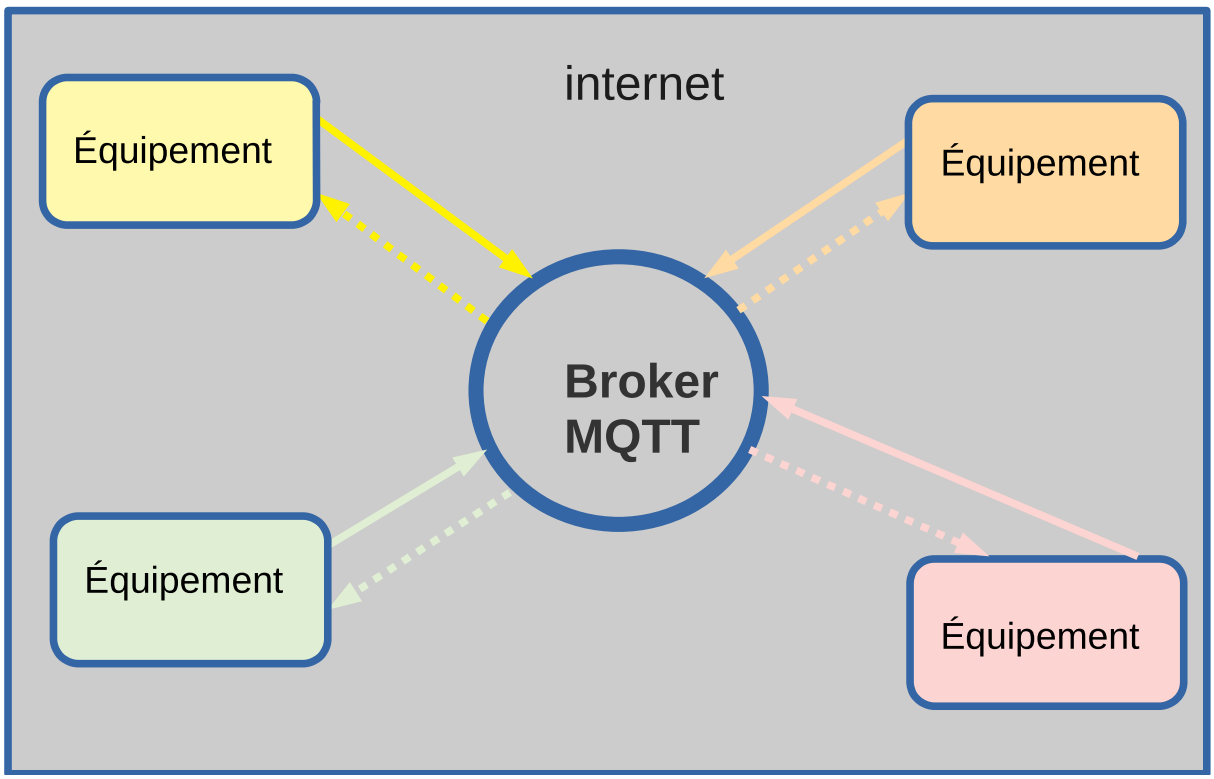
Ce type de réseau permet de faire communiquer très simplement des appareils entre eux, par exemple des objets connectés avec une faible puissance de calcul contrôlés avec un smartphone.

2.3.3.7.1 Principe du service rendu

Les figures ci-dessous illustrent le principe du service rendu.

Tous les équipements et le broker sont reliés à l'internet.

Le Broker joue un rôle équivalent à celui de twitter. Chaque équipement peut émettre des messages sur des flux particuliers et écouter les flux émis par les autres équipements.



Ce système permet à des équipements de s'envoyer et de recevoir des messages de manière simple et selon un mode de communication point à multipoint. Voir figure ci-dessous.

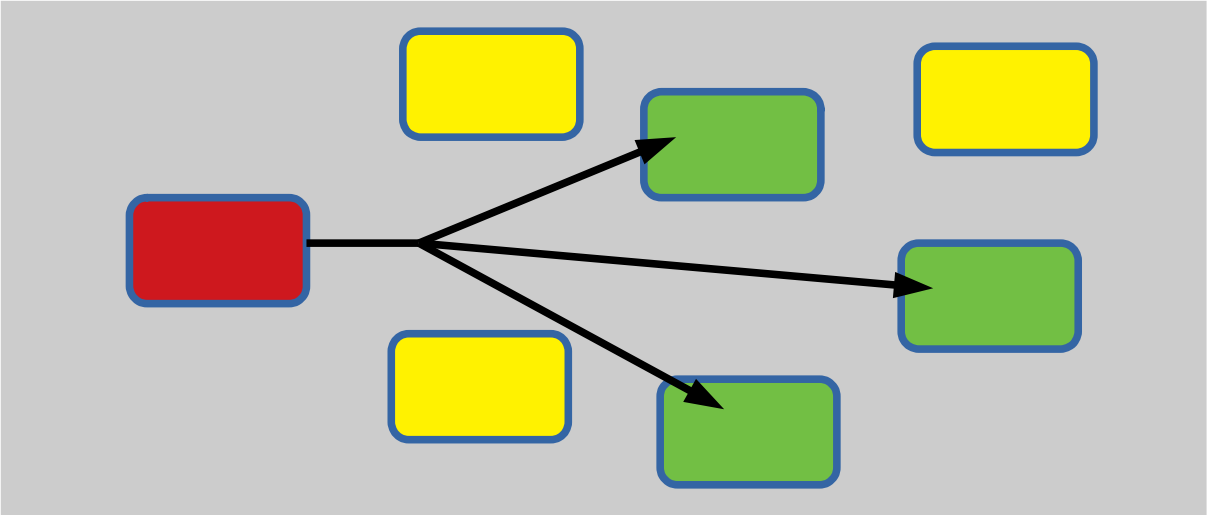


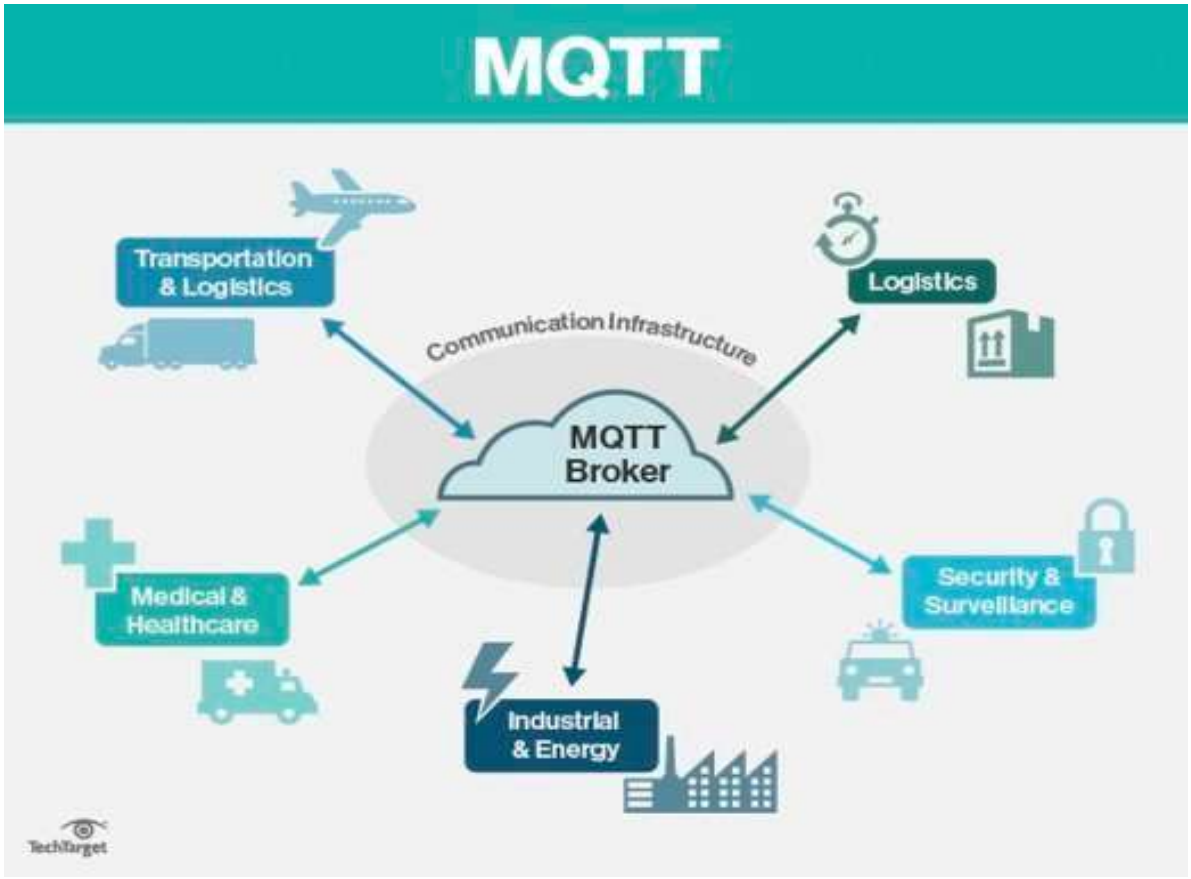
Illustration 32: MQTT Broker principe du service rendu

Cette figure présente une communication point à multipoint. L'équipement rouge envoi un message qui est reçu simultanément par chacun des équipements verts qui se sont abonnés au flux.

2.3.3.7.2 Cas d'emploi du service MQTT

La figure ci-dessous illustre différents cas d'emplois possibles du service MQTT. Source : TechTarget.

.



2.3.3.7.3 Concepts de base du protocole MQTT

MQTT signifie : **M**essage **Q**ueuing **T**elemetry **T**ransport

Pour bien comprendre les concepts de base du système, nous allons développer les quelques points suivants :(source : randomnerdtutorials.com)

- Publish et Subscribe (i.e Publication/Souscription)
- Messages
- Topics
- Broker

2.3.3.7.3.1 Publication/Souscription

Un équipement (c'est à dire un objet connecté, par exemple : smartphone, interrupteur, service météo, jardin connecté) peut publier (publish) un message sur un « topic » . Le mot topic est équivalent au mot : flux.

Un équipement doit s'abonner à un topic particulier pour recevoir des messages envoyés sur ce topic.

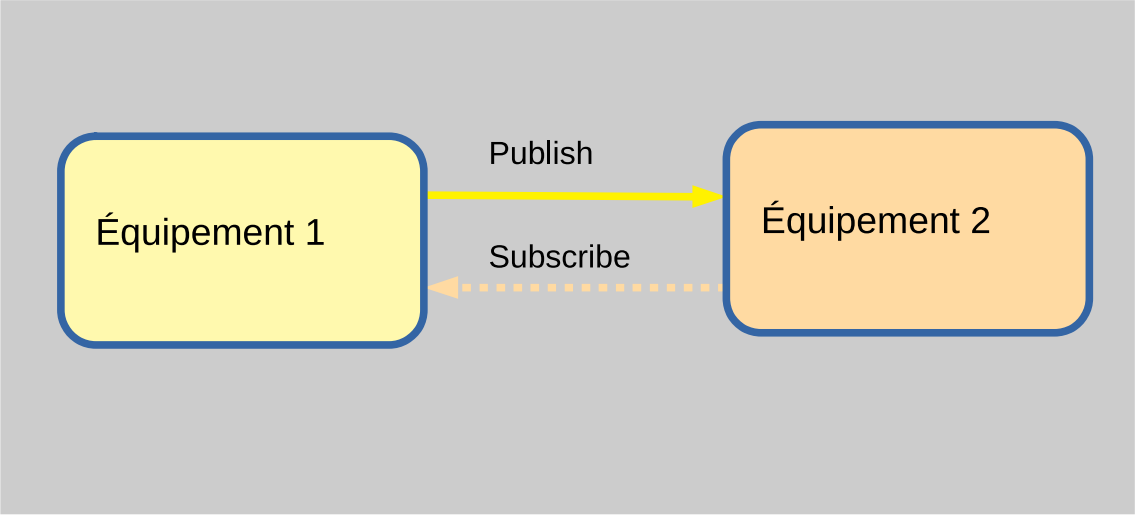


Illustration 33: MQTT Publication/Souscription

- Par exemple, L'équipement 1 publie sur un topic intitulé : *temperature/cuisine,*
- L'équipement 2 souscrit (i.e s'abonne) à ce topic : *temperature/cuisine,*
- ainsi, l'équipement 2 reçoit les messages envoyés par l'équipement 1 sur ce topic.
- Tout autre équipement peut aussi s'abonner sur le topic temperature/cuisine et ils recevront tous , en même temps, le message envoyé par l'équipement 1.
- L'équipement 1 peu publier d'autres messages sur d'autres topics et s 'abonner à plusieurs autres topics.

2.3.3.7.3.2 Messages

Les messages sont les informations échangés entre les équipements Un message contient par exemple : une commande ; « monter la température », ou des données ; « la température actuelle est de 12°C ».

2.3.3.7.3.3 Topics

Un topic correspond à un flux d'information. Un topic est représenté par

des chaînes de caractères espacées par « / » . Par exemple :

jardin/humidité

2.3.3.7.3.4 Broker

Le Broker assure :

- la réception de tous les messages associés à leur topic respectifs et
- le renvoi simultané de ces messages vers les clients qui ont souscrit à ces topics.

2.3.3.7.4 MQTT : un protocole de communication pour les objets connectés

Source : ici

Les principales caractéristiques du protocole MQTT sont :

- Il est agnostique quant aux informations qu'il permet de faire transiter, c'est uniquement un protocole de transport pour les objets connectés. La taille maximale du ''payload '' d'un message est de 256Mo
- Sa légèreté : n'augmente que légèrement la consommation de bande passante
- Il permet de contrôler facilement la fiabilité de transmission des informations
- Il constitue une abstraction pour la gestion du réseau : pour des connexions instables, la gestion des déconnexions/reconnexions est simplifiée
- Il permet à de nombreux clients de recevoir ou de diffuser une information
- Le chiffrement via TLS/SSL
- La possibilité de gérer quels clients ont le droit d'accéder à une information ou de la publier

2.3.3.7.5 Quelques exemples de Brokers

Source : ici (en Anglais)

Il existe de nombreux types de brokers et de sites web associés. La documentation Wikipédia ici (en Anglais) en présente les principales implémentations.

L'un des points important à retenir est que le protocole MQTT est un standard ISO. Ceci signifie par exemple que dans un système basé sur MQTT, il est toujours possible de changer de Broker.

Le Broker le plus utilisé est Mosquitto et c'est celui que nous utiliserons dans nos travaux pratiques.

2.3.3.7.6 Broker MQTT et Sécurité

source : ici (en Anglais)

2.3.3.7.6.1 Les contraintes

Dans un système basé sur MQTT il est possible d'implémenter les mécanismes de sécurité présentés précédemment au chapitre ici.

Le document ici (en Anglais), en présente les possibilités dans le contexte MQTT.

Néanmoins, la mise en place de ces mécanismes est contraint par le manque ,en général, de puissance de calcul des équipements, en particulier pour chiffrer et déchiffrer. A cette date, la plupart des clients MQTT ne disposent pas de cette puissance.

En conclusion, les possibilités de sécurisation des systèmes MQTT existent mais elles ne sont pas mises en œuvre en général par manque de puissance de calcul dans les clients.

2.3.3.7.6.2 Exemple de solution de sécurité : installer le Broker en zone privée

Il est néanmoins possible de sécuriser un système MQTT en installant le broker en zone privée, c'est à dire dans un environnement sécurisé.

La figure suivante en présente le principe.

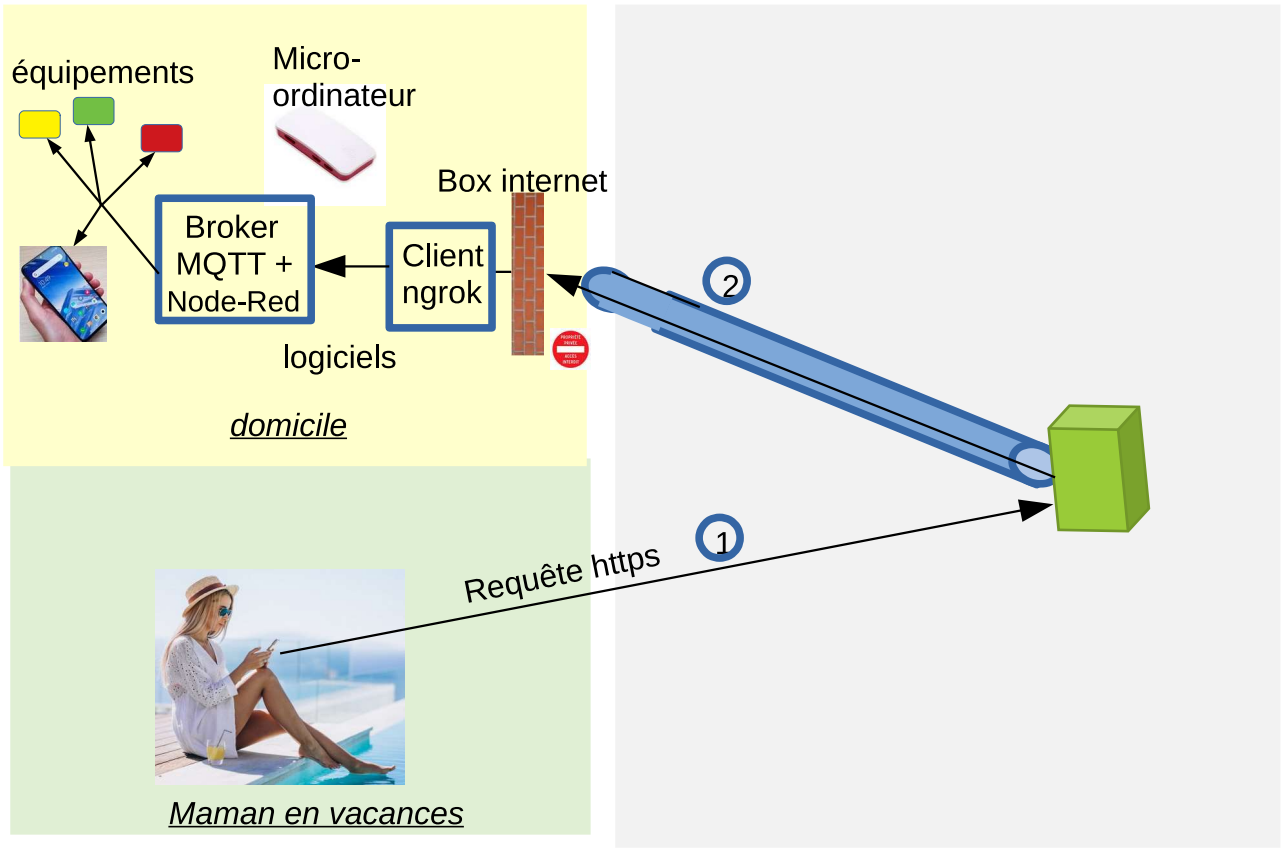


Illustration 34: Exemple de solution de sécurité : installer le Broker en zone privée

Le Broker MQTT est placé en zone privée, c'est à dire au domicile par exemple.

La Box internet interdit « de base » toute demande de connexion émise depuis l'extérieur vers les équipements de la zone privée.

La connexion client ngrock – site ngrock est permanente et établie à l'initiative du client ngrock.

Pour avoir accès aux équipements MQTT du domicile, la « maman en vacances » se connecte en https au site web ngrok.

Le client ngrock et le Broker MQTT sont installés dans un micro ordinateur, par exemple : Raspberry, en fonctionnement permanent.

2.3.3.7.7 Démonstrations du service MQTT

2.3.3.7.7.1 Demonstration MQTT N°1 : test du réseau MQTT au niveau local

Configuration :

1xRasperry pi + 2 terminaux client MQTT sur PC (linux ou windows)

Création d'un client MQTT qui écoute sur le topic 'sensor/temperature'

1) Depuis un terminal linux ou windows (putty), se connecter au raspberry pi qui héberge le broker mosquitto en utilisant l'une des commandes suivantes :

ssh pi@192.168.1.27 (sur linux)

putty : user = pi, IP = 192.168.1.27 (sur windows)

2) entrer la commande suivante :

pi@raspberrypi:~ $ mosquitto_sub -d -t sensor/temperature

Cette commande lance un client MQTT qui écoute sur le topic 'sensor/temperature'

Création d'un client MQTT qui publie sur le topic 'sensor/temperature'

1) Depuis un terminal linux ou windows (putty), se connecter au raspberry pi qui héberge le broker mosquitto en utilisant l'une des commandes suivantes :

ssh pi@192.168.1.27 (sur linux)

putty : user = pi, IP = 192.168.1.27 (sur windows)

2) entrer la commande suivante :

pi@raspberrypi:~ $ mosquitto_pub -d -t sensor/temperature -m 18.3

Cette commande envoie la valeur de température : '18.3' sur le topic 'sensor/temperature'

vérifier que la valeur de la température : 18.3 est bien reçue sur le terminal qui écoute sur le topic 'sensor/temperature'

relancer la commande pour vérifier le bon fonctionnement de ce test.

2.3.3.7.7.2 Demonstration MQTT N°2 : test du réseau MQTT en y accédant depuis un réseau publique (c'est à dire depuis n'importe où)

Cette démonstration reprend la même procédure que celle précédente. La seule différence est que la connexion (ssh) des terminaux avec le raspberry pi passent par le vpn ngrok.

Configuration :

1xRasperry pi + **3** terminaux client MQTT sur PC

Création du VPN ngrok

Depuis un terminal , entrer la commande :

./ngrok tcp 22 (à partir d'un terminal sur raspberry pi)

La réponse renvoyée contient par exemple :

Forwarding tcp://0.tcp.ngrok.io:14659 -> localhost:22

cette réponse signifie que pour se connecter au raspberry pi selon le protocole ssh , on effectue la commande :

ssh pi@0.tcp.ngrok.io -p 14659 (sur linux)

putty : user = pi, IP = 0.tcp.ngrok.io, port= 14659 (sur windows)

Création d'un client MQTT qui écoute sur le topic 'sensor/temperature'

1) Depuis un terminal linux ou windows (putty), se connecter au raspberry pi qui héberge le broker mosquitto en utilisant l'une des commandes suivantes :

ssh pi@0.tcp.ngrok.io -p14659 (sur linux)

putty : user = pi, IP = 0.tcp.ngrok.io, port= 14659 (sur windows)

2) entrer la commande suivante :

pi@raspberrypi:~ $ mosquitto_sub -d -t sensor/temperature

Cette commande lance un client MQTT qui écoute sur le topic 'sensor/temperature'

Création d'un client MQTT qui publie sur le topic 'sensor/temperature'

1) Depuis un terminal linux ou windows (putty), se connecter au raspberry pi qui héberge le broker mosquitto en utilisant l'une des commandes suivantes :

ssh pi@0.tcp.ngrok.io -p14659 (sur linux)

putty : user = pi, IP = 0.tcp.ngrok.io, port= 14659 (sur windows)

2) entrer la commande suivante :

pi@raspberrypi:~ $ mosquitto_pub -d -t sensor/temperature -m 18.3

Cette commande envoie la valeur de température : '18.3' sur le topic 'sensor/temperature'

relancer la commande pour vérifier le bon fonctionnement de ce test.

2.3.3.7.7.3 Demonstration MQTT N°3: accèder à son réseau MQTT depuis n'importe où avec l'outil Node-Red

Nota : cette démonstration sera faite après prise de connaissance du chapitre suivant : « Node Red programmation graphique pour objets connectés »

Cette démonstration utilise la configuration suivante : 1xRasperry pi + smart-phones et PCs

2.4 Les services de pilotage automatique dans le monde connecté

2.4.1 Node Red

2.4.1.1 Qu'est-ce que Node Red ?

ref

Node-RED est un outil logiciel graphique de type ‘programmation événementielle’.

La figure ci-dessous illustre son fonctionnement.

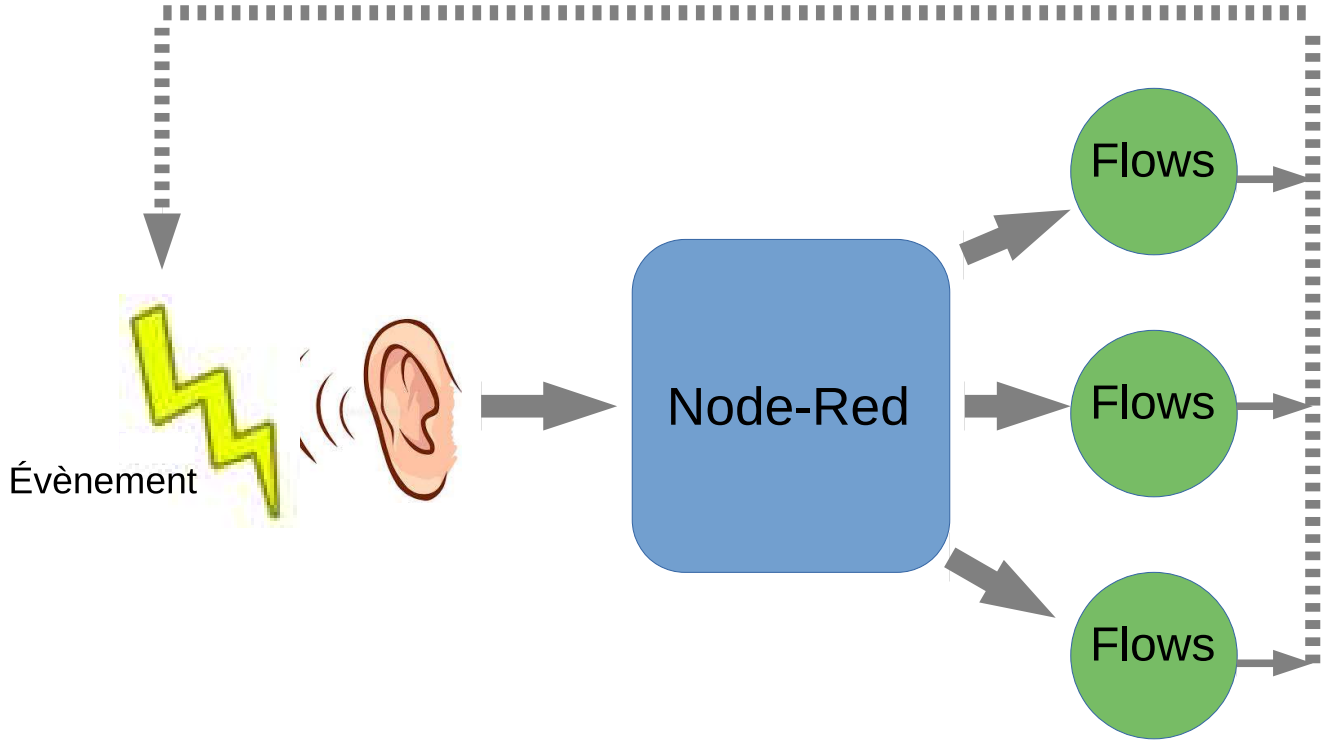


Illustration 35: Node-Red: illustration de son fonctionnement

2.4.1.1.1 Principe de fonctionnement de Node-Red

Lorsque Node-Red reçoit un évènement, celui ci est pris en charge par un ou plusieurs ‘flows’ (flux).

Un ‘flow’ (flux en Français) est constitués de blocs fonctionnels (i.e programme) apparaissant comme des ‘briques’ de fonctions. Les ‘flows’ prennent en charge les évènements et lancent les actions appropriées au traitement de ces évènements.

Ces actions peuvent , à nouveau , si nécessaire, déclencher un/des nouveaux événement(s) et ainsi de suite.

Les ‘flows’ sont des processus qui fonctionnent en simultanéité.

2.4.1.1.2 La programmation de Node-Red

voir : prise en main de Node-Red

La programmation s’effectue par assemblage de blocs fonctionnels. Node-red permet de développer des objets connectés (et beaucoup d’autres choses). On programme avec **Node-RED** en liant des fonctions présentées sous la forme de briques. Le flux de données passe d’un traitement à l’autre (d’une fonction à l’autre). Certaines fonctions proposent des paramètres qu’il suffit de définir à l’aide d’une liste de choix ou d’un champ à remplir (par exemple un clé d’API pour un service météo). Il existe plusieurs centaines de plugins dans tous les domaines : enregistrer les données sur une base de données (MySQL, MongoDB…), piloter les E/S d’un Arduino ou d’un Raspberry , ajouter une interface graphique (UI) pour tracer des graphiques, afficher des jauges, commander un relai à l’aide d’un bouton…

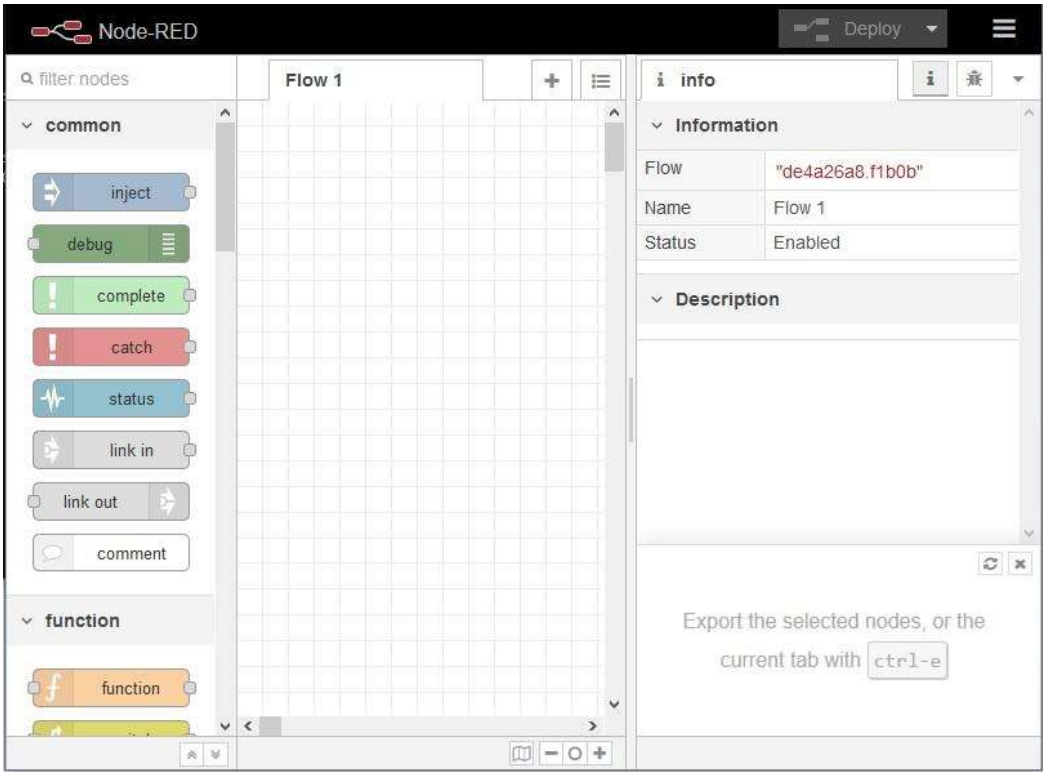


Illustration 36: écran de démarrage de Node-RED

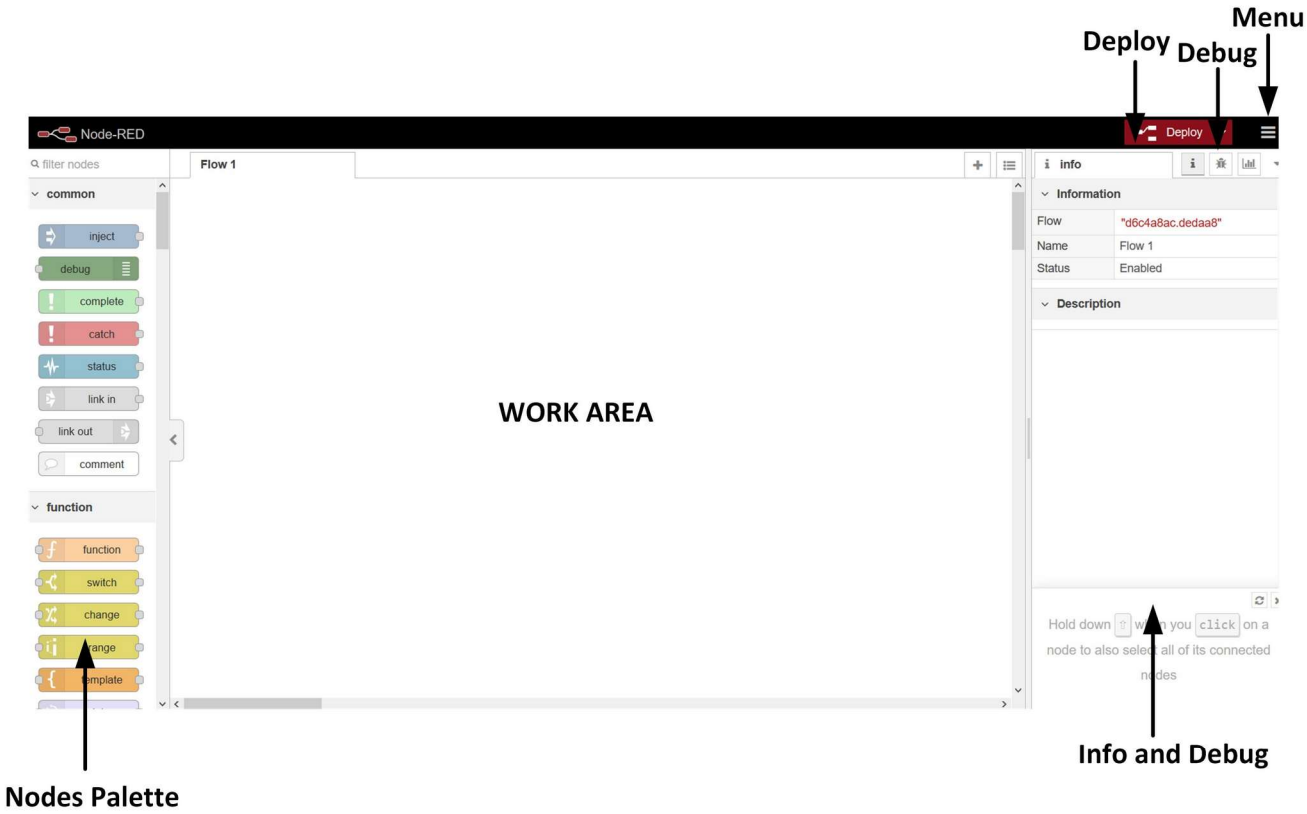


Illustration 37: Explication de l'écran de démarrage de Node-RED

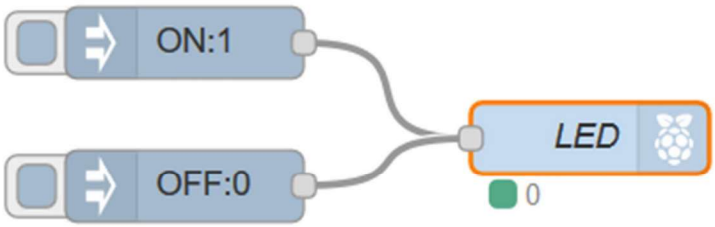


Illustration 38: Node-Red : Diagramme d'un 'flow'

2.4.1.1.3 Pérennité et popularité de Node-red

Node-Red est un projet Open Source (et gratuit) soutenu par IBM et par l'OpenJS Foundation.

Le code de Node-Red est accessible sur le site GitHub. GitHub héberge les logiciels libres.

La taille de la librairie Node-red (voir https://flows.nodered.org/) témoignent qu'il dispose d'une forte communauté.

Travaux pratiques :

S'inspirer de : ref1, ref2, ref3

2.4.1.1.4 Node Red nécessite t'il des connaissances pointues en programmation ?

Ref : https://www.automation-sense.com/blog/automatisme/node-red-francais.html

Avec Node-RED,l'utilisateur n'a pas vraiment besoin d'avoir des connaissances pointues en programmation,l'ensemble de sa conception de programme s'effectue en reliant et en paramétrant des blocs de code.

Node-RED a plusieurs avantages parmi lesquels on peut citer :

- Il réduit le temps nécessaire pour créer une application fonctionnelle.
- Il est accessible à un large éventail de développeurs et de non-développeurs.
- La nature visuelle de l'interface le rend très intuitif
- Il dispose d'une forte communauté et par conséquent il existe une panoplie de bibliothèques Node-RED

2.4.1.2 Node Red pour connecter tout type d'objets, ceux du commerce et ceux que nous avons fabriqués

2.4.1.2.1 Node Red permet de gérer la plupart des objets connectés récents du commerce.

Voir quelques exemple aux liens ci-après.

Tplink

netatmo, netatmo-cameracontrol

Arduino (serial usb)

fitbit

ezviz

viseo

tahoma

nest

tado-client, tado

huemagic

xiaomi-device, xiaomi-devices, xiaomi-smart-devices, xiaomi-sensors, xiaomi-ble

2.4.1.2.2 Node Red pour connecter son smart phone en tant qu'objet connecté

Voir ces liens : Node red sur android, Termux:API , remote-xy, video1 node red on Android, video 2 node red on Android , Que faire avec node red sur Android ?

Pour installer l'application : cliquer ici

2.4.1.2.3 Node Red pour se connecter à IFTTT

Voir ce lien .

2.4.1.2.4 Node Red , interface Cloud

Voir ces liens :

https://flows.nodered.org/ , https://youtu.be/19DniKv2ggw

2.4.1.2.5 Node Red , interface Arduino série

https://youtu.be/nJ1wtUtcLfM

2.4.2 Domoticz

Références :

Site domoticz; https://www.domoticz.com/wiki/Main_Page (en Anglais)

https://www.jipitech.com/domoticz-presentation-de-la-solution-domotique-pour-tous

2.4.2.1 Qu'est-ce que Domoticz ?

Domoticz est une solution domotique gratuite et open source, consommant très peu de ressources système, et pouvant être ainsi installée sur différents matériels et systèmes d'exploitation (Linux - Windows - Mac - Raspberry Pi - NAS Synology - FreeNAS).
On accède à son interface par l'intermédiaire d'une application (disponible sur iOS et Android) ou d'un navigateur internet. De plus le système est compatible avec tous les navigateurs (excepté Internet Explorer qui nécessite la version 10 minimum), et s'adapte aux formats tablettes et mobiles

On peut aisément personnaliser l'interface de Domoticz, celle-ci étant au format HTML5.

Domoticz est compatible avec de nombreux matériels et protocoles.
La liste est longue, citons simplement quelques-uns : RFXCOM, RFLink, Z-Wave, EnOcean, Fibaro, Philips Hue, Caméras IP...
La liste complète est disponible sur le Wiki de Domoticz : Hardware

2.4.2.2 Domoticz pour connecter tout type d'objets, ceux du commerce et ceux que nous avons développés

Domoticz permet de développer des services de pilotage automatique qui inclue tout type d'objets connectés : ceux du commerce et ceux que nous avons développés. La figure ci-après en expose le principe. Voir le lien : https://www.domoticz.com/wiki/MQTT#MQTT_to_Domoticz pour présentation détaillée.

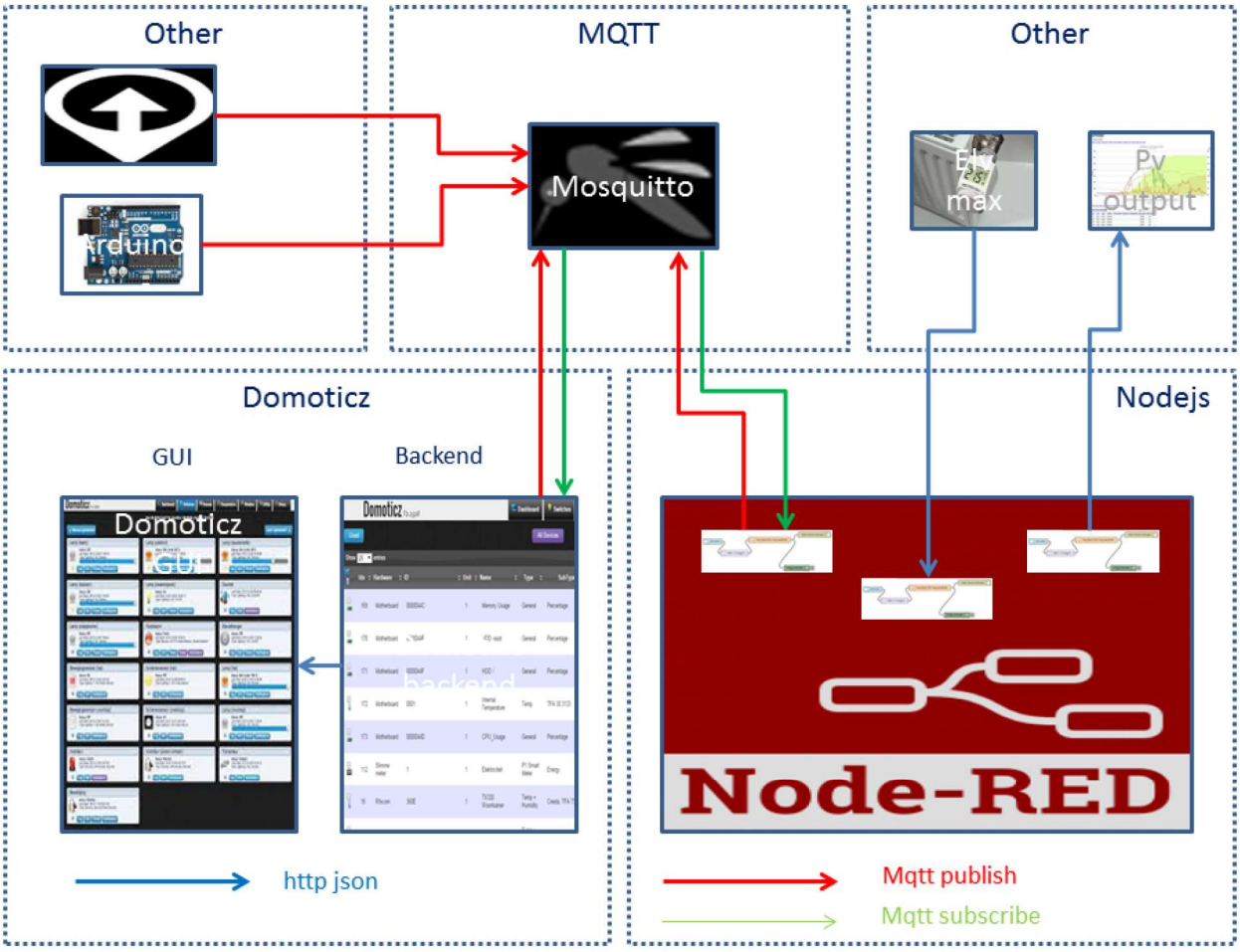


Illustration 39: Domoticz pour connecter tout type d'objets, ceux du commerce et ceux que nous avons développés

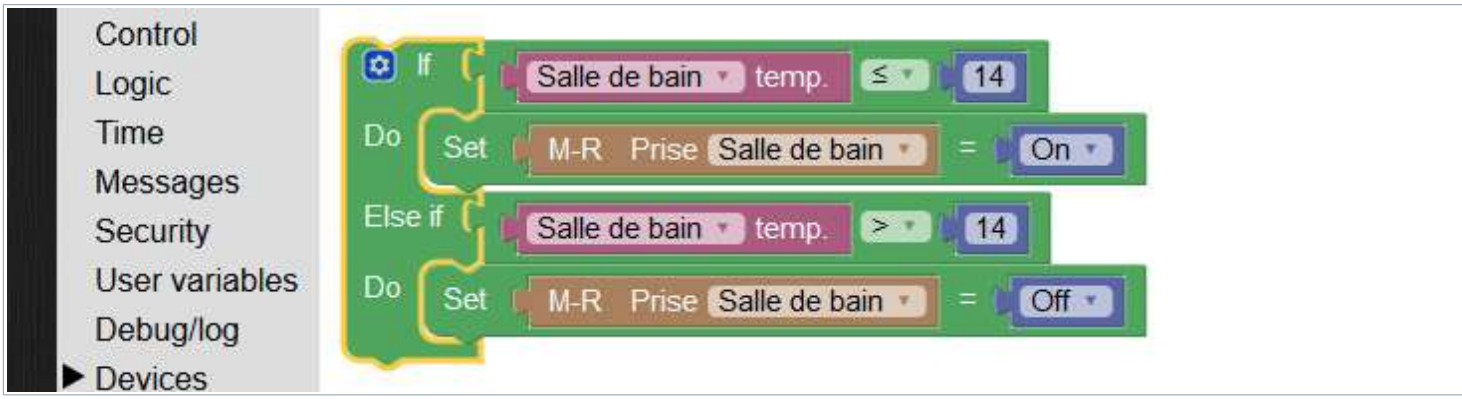
2.4.2.3 Que peut-on faire avec Domoticz ?

Bien des choses. Grâce à sa gestion de modules domotiques, les possibilités sont très entendues.

- •Contrôler divers appareils : interrupteurs, prises, volets roulants, portails, chauffages, lumières, thermostats etc.
- •Surveiller : capteurs de température, mouvement, luminosité, d'humidité, incendies, caméras, stations météo etc.
- •Afficher diverses informations : température, luminosité, pluviométrie, vitesse du vent, consommation d'électricité, de gaz ou d'eau etc.

•Recevoir automatiquement des notifications sur son mobile ou par mails (lors d'une fuite d'eau, de température trop élevée, de fenêtre mal fermée...)
•Concevoir des scénarios : le chauffage s'allume si la température descend en dessous de 19 °C et si nous sommes entre 17 et 21h, fermer les volets si la température extérieure dépasse 21 °C et si la luminosité est forte...

On peut utiliser des scripts plus ou moins complexes pour créer des scénarios divers. Cela peut se faire graphiquement, pour des évènements relativement simples, par l'intermédiaire de blocs prédéfinis, grâce à la bibliothèque logicielle Blockly. Il suffit alors d'assembler des sortes de pièces de puzzle pour créer un scénario.



Pour des évènements plus complexes, on passera alors à la programmation pure et dure en langage de script Lua.

2.4.2.4 Liste des objets connectés du commerce gérés par Domoticz

Domoticz permet de gérer la plupart des objets connectés du commerce.

Voir Wiki-Domoticz/Hardware (en Anglais).

2.4.2.5 Comment utiliser Domoticz ?

Comme un système domotique se doit d'être disponible 24h sur 24, et Domoticz étant peu gourmand en ressources système, le support idéal est sans conteste le nano-ordinateur Raspberry Pi, bon marché et lui-même très peu glouton en consommation électrique (voir Raspberry pi : présentation)

2.4.2.6 Liens

Le site officiel : Domoticz (en anglais).
Le Wiki de domoticz (en anglais).
Le forum officiel.

Liens pour l'installation de Domoticz :
Domoticz sur Raspberry Pi : installation pas à pas – Partie 1/2
Domoticz sur Raspberry Pi : installation pas à pas – Partie 2/2

2.5 Synthèse des découvertes et explorations futures

Ce chapitre a pour objectif de présenter

- une synthèse des principales découvertes de ce cours
- et les activités futures qui seront probablement proposées au club

2.5.1 Les découvertes faites dans ce cours

La principale découverte faite dans ce cours, c'est que nous pouvons assez facilement mettre en place des services pour, par exemple :

- Je m'absente (de mon domicile , de mon travail..) alors…(mise en place des sécurités par exemple...)
- Je rentre chez moi..
- Je me soigne…, je surveille ma santé...Je surveille et aide ma mère qui est en maison de retraite...
- Je vais me coucher…, je me réveille
- La météo va devenir dangereuse...alors...(je rentre les stores..)
- Il fait nuit alors…, il fait jour alors…
- je surveille et entretien...mon jardin, ..mes animaux domestiques...

Ces services peuvent être étendus à l'échelle mondiale car nous avons découvert comment étendre une zone privée au niveau mondial avec des outils tels que ngrok et le broker MQTT.

Pour mettre en place ces services, les découvertes faites dans ce cours sont:

- La découverte des notions de base du monde connectée et son vocabulaire.
- La découverte de la sécurité dans le monde connecté et de ses applications, en particulier le VPN, le HTTPS, la blockchain.
- La découverte de la découpe du monde connecté en zones privées et zone publique
  - La zone publique correspond à l'ensemble des des sites internet : sites web et autres types reliés au réseau mondial internet
  - des zones privées, par exemple : le domicile, l'ensemble des appareils que l'on porte sur soi à l'extérieur, les établissements d'entreprise, les commerces.

    Ces zones privées sont constituée d'objets connectés : smart phone, montre connecté, box internet, lampes connectées, Interrupteurs connectés, enceintes connectées, d'aspirateurs, de robots...

    Au moins l'un des objets connecté dans une zone privée joue le rôle de 'Box IOT'. Cette 'Box IOT' est par exemple un mini PC tel que le Raspberry pi ou un smart phone Androïd, ou 'la box IOT' d'un fournisseur, par exemple une enceinte connecté...

    Les zones privées sont protégées contre les intrusions provenant de l'extérieur. L'équipement qui assure cette protection est la 'box internet' en intérieur ou 'le smartphone' que l'on porte sur soi en extérieur.
- La découverte de types de sites internet qui permettent de relier les zones privées entre elles et ainsi créer des zones privées étendus. Les sites découverts sont :
  - ngrok
  - les brokers MQTT
- La découverte d'outils permettant de créer des scénarios en mettant en place des liaisons entre des sites internet, des objets connectés, des fonctions , des applications pour nous rendre des services. Les principaux outils découverts sont Node Red et IFTTT. Ces outils sont complémentaires : Node Red peut utiliser IFTTT et inversement.
  - Node Red

    Node Red permet de créer des services. Ceux-ci peuvent être complètement automatique ou commandés depuis un smart phone par exemple.

    Les objets connectés peuvent être des objets du commerce et des objets connectés fabriqués.

- IFTTT

  IFTTT offre des services de type ‘si ceci alors faire cela’ en reliant innombrables sites internet

2.5.2 Les explorations futures envisagées au club (à confirmer)

Suite à ces premières découvertes du monde connectés, les nouvelle activités envisagées au club sont :

Ateliers découverte des objets connectés. Par exemple : séance de découverte d’un scénario mettant en œuvre une lampe, une prise connecté et une enceinte connectée.

Ateliers exploration du monde connecté mettant en œuvre : les objets connectés du commerce, les objets connectés fabriqués, une/des ‘box iot’ basé sur Raspberry ou sur smartphone android, les outils : Node Red, ngrok et broker MQTT

Ateliers fabrication d’objets connectés. Plusieurs type d’ateliers, par exemple :

ateliers basés sur cartes ESP32 ou cartes ESP8266

ateliers basés sur raspberry pi

En parallèle à ces activités, mise en place d’une activité:

Assistance Monde et Objets Connecté aux Adhérents , Forum

2.5.3 Plateforme Monde Connectée (MC)

Pour ces explorations futures, l’une des activités envisagée est de créer une plateforme MC (Monde connecté) conforme au modèle étendu présenté au chapitre #Découvertes des services étendus.

2.5.3.1 Présentation préliminaire de la plateforme MC

La figure ci-dessous est une vue générale de cette plateforme

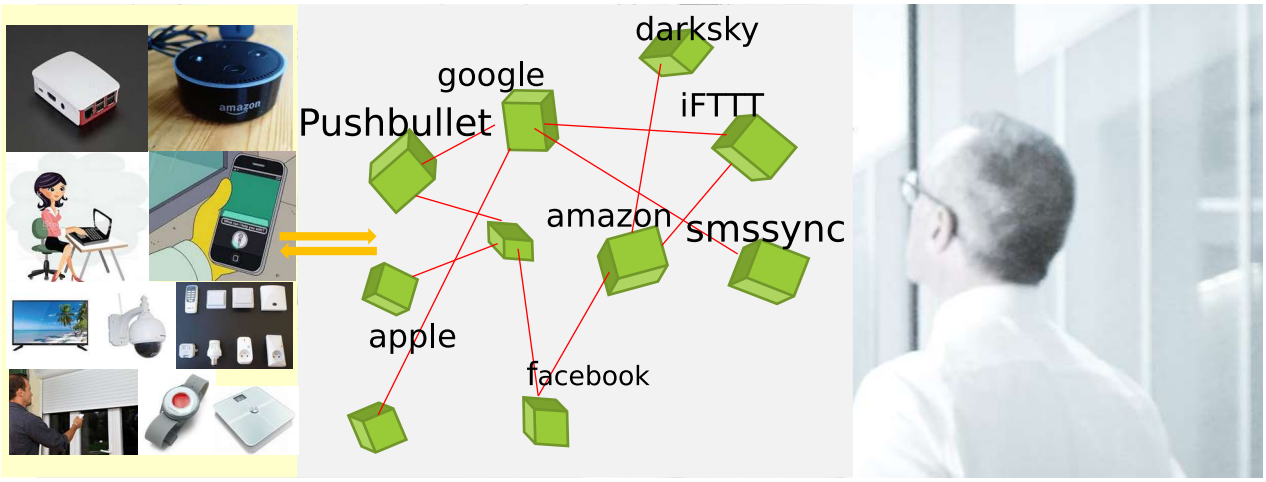


Illustration 40: Illustration du monde connecté dans le contexte des services étendus

Par exemple, nous y trouvons les objets connectés suivants :

- un micro ordinateur
- une enceinte vocale Alexa
- un ordinateur portable
- un smart phone
- 2 camera de surveillance : l'une basée sur le matériel Raspberry, l'autre issue du commerce
- des équipements domotiques divers
- des volets roulants connectés (simulé)
- des objets connectés du commerce
- des objets connectés que j'ai fabriqué au club

Cette plateforme permettra en particulier de démontrer les points suivants abordé dans ce cours :

- Modèle du monde connecté étendu
- Je reçois un sms lorsque mon enfant rentre de l’école
- Je dépanne mon enfant qui a perdu la télécommande des volets
- Je commande mes appareils depuis n'importe où par la voix
- Depuis mon lieu de vacance, Je contrôle que tout va bien à la maison